

IBM Lotus Protector for Mail Security



Administratorhandbuch

Version 2.8 Release 2.8.1

Copyrightvermerk

© Copyright IBM Corporation 2006, 2013.

Ausgabe Oktober 2013

Diese Veröffentlichung ist eine Übersetzung des Handbuchs
IBM Lotus Protector for Mail Security, Administrator's Guide, Version 2.8.1,
IBM Form SC27-3829-01,
herausgegeben von International Business Machines Corporation, USA

© Copyright International Business Machines Corporation 2006, 2013

Informationen, die nur für bestimmte Länder Gültigkeit haben und für Deutschland, Österreich und die Schweiz nicht zutreffen, wurden in dieser Veröffentlichung im Originaltext übernommen.

Möglicherweise sind nicht alle in dieser Übersetzung aufgeführten Produkte in Deutschland angekündigt und verfügbar; vor Entscheidungen empfiehlt sich der Kontakt mit der zuständigen IBM Geschäftsstelle.

Änderung des Textes bleibt vorbehalten.

Herausgegeben von:
TSC Germany
Kst. 2877
Oktober 2013

Inhaltsverzeichnis

Tabellen.	v
------------------	----------

Informationen zu dieser Veröffentlichung vii

Neuigkeiten in Version 2.8	vii
Technische Unterstützung.	ix
Lotus Protector for Mail Security Mit einer Befehlszeile verwenden	ix

Kapitel 1. Erste Schritte mit Lotus Protector Manager. 1

Im Lotus Protector Manager navigieren	1
Startseite.	3
Schutzstatus	3
Bewertungsstatus.	4
Datenverkehrsstatus	5
Ressourcenstatus	5
Status der Updates	6
Systemstatus	7
Abschnitt A: Empfohlene Tasks	8
Lizenzschlüssel installieren	8
Konfigurationseinstellungen sichern	9
Updates für E-Mail-Sicherheit ausführen.	10
Lokale Firewall konfigurieren	10
E-Mail-Adressen für Administratoren und von Accounts für Systembenachrichtigungen definieren	11
Abschnitt B: Optionale Tasks	12
Kennwörter für Lotus Protector for Mail Security ändern	12
Einstellungen für Datum und Zeit ändern	13
ICAP-kompatiblen Clients Virenskanservices in Echtzeit bereitstellen	14
Netzschnittstellen verwalten.	14
Netzübertragungen weiterleiten	16

Kapitel 2. SMTP-Konfiguration 19

Lotus Protector for Mail Security implementieren.	19
Einstellungen für den SMTP-Service konfigurieren	23
Allgemeine Einstellungen für den SMTP-Service konfigurieren.	23
Einstellungen für Transport Layer Security (TLS) konfigurieren.	26
IP-Adressen für lokale Domänen und Relay-Hosts definieren.	27
Globale IP-Zugriffsliste konfigurieren.	28
DNSBL-Einstellungen konfigurieren	29
Empfängerüberprüfung konfigurieren	30
Analyse der Nullebene (ZLA, Zero Level Analysis) aktivieren	31
Dynamischen Hostreputationsfilter konfigurieren.	33
Ausgehende E-Mail-Nachrichten aus Ihrem Netz einrichten	35

Unzustellbare E-Mail-Nachrichten und SMTP-Protokolldateien aus dem Dateisystem entfernen.	38
Installation von TLS-Zertifikaten	39
SMTP-TLS-Zertifikate hochladen	40
TLS-Verbindung testen	42
SMTP-Warteschlangen.	43
E-Mail-Datenverkehr in den Zustellungswarteschlangen überwachen.	44

Kapitel 3. Richtlinienkonfiguration 47

Informationen zu Richtlinienregeln	47
Who-Objekte	49
Who-Objekte überprüfen	50
When-Objekte	51
Bedingungsobjekte	52
Analysemodule	53
Spamanalysemodule verwenden	57
Response-Objekte	57
Verzeichnisobjekte	59
Zeitplanobjekte	62
FTP-Server	63
Nachrichtenspeicher	64
In einem Nachrichtenspeicher nach Nachrichten suchen	65
Quarantänebericht inaktivieren	66
Schablone für Quarantänebericht	67
Empfänger eines Quarantäneberichts definieren	69
Inhalte der Dateien überprüfen, die eingehenden E-Mail-Nachrichten angehängt sind	70
DNSBL-/Spamdatenflusseinstellungen konfigurieren	71
Zugriffsberechtigungen für die Endbenutzerschnittstelle einrichten	72
E-Mail-Nachrichten verfolgen	73

Kapitel 4. Benachrichtigungen, Systemereignisse und Protokolle. 75

E-Mail-Benachrichtigungen und SNMP-Statusmeldungen verwenden.	75
Empfänger von Statusmeldungen definieren	77
Erweiterte Parameter für die Ereignisbenachrichtigung konfigurieren.	77
Systembezogene Ereignisse verwalten	79
Protokolldateien anzeigen	80
Diagnosedatei generieren.	80
Protokolldateien zum Ermitteln der Ursache einer blockierten E-Mail-Nachricht anzeigen	80

Kapitel 5. Vordefinierte Berichte 81

Vordefinierte Berichte	81
Vordefinierten Bericht generieren	82
Zeitplanung bei der Ausführung von vordefinierten Berichten	82

Kapitel 6. Sicherung und Wiederherstellung 85

Sicherungsarten	85
Konfigurationseinstellungen sichern	86
Vollständige Systemsicherungen erstellen	87

Kapitel 7. Updates 89

Aktuellen Status und Lizenzen für den Spamschutz anzeigen	89
Aktualisierungsprozess automatisieren	90
Ereignisbenachrichtigung für Updates konfigurieren	92
Erweiterte Parameter für automatische Updates konfigurieren	93

Anhang A. Endbenutzerschnittstelle . . . 95

Zugriffsberechtigungen für die Endbenutzerschnittstelle einrichten	95
Benutzeraccounts für Endbenutzerschnittstelle verwalten	97
Erweiterte Parameter für die Endbenutzerschnittstelle konfigurieren	97

Anhang B. Mail Security-Cluster 99

Informationen zu Mail Security-Clustern	99
Neuen Mail Security-Cluster erstellen	100
Mit vorhandenem Mail Security-Cluster verbinden	101
Kennphrasen oder IP-Adressen für den Mail Security-Cluster ändern	102
Client aus dem Mail Security-Cluster entfernen	102
Cluster von Mail Security-Systemen löschen	103

Anhang C. Integration in Lotus Domino 105

Serverkonfiguration für Lotus Domino	105
Richtlinie des Domino-Administratordesktops konfigurieren, um die Integration zu ermöglichen	105
Konfiguration von Lotus Protector for Mail Security	106
Zugriffsberechtigungen für Lotus Notes-Benutzer aktivieren	106
Benutzerauthentifizierung über Ihren Lotus Domino-Server aktivieren	107
Fehlerbehebung für die LDAP-Verbindung zu Ihrem Lotus Domino-Server	107

Anhang D. Erweiterte Parameter 109

Allgemeine erweiterte Parameter	109
Erweiterte Parameter für LDAP-Server	110
Erweiterte Parameter für Nachrichtenspeicher	111
Erweiterte Parameter für SMTP-Einstellungen	112
Erweiterte Parameter für die DNSBL-Einstellungen	113
Erweiterte Parameter für eine Clusterreplizierung	113
Erweiterte Parameter für die Endbenutzerschnittstelle	114

Anhang E. Die Funktionen zur behindertengerechten Bedienung erfordern Lotus Protector for Mail Security. 115

Bemerkungen 117

Marken	118
------------------	-----

Index 119

Tabellen

1. Neue Funktionen für Lotus Protector for Mail Security V2.8	vii	19. Who-Objekte überprüfen	50
2. Kategorien der Navigationsstruktur	1	20. Bedingungsobjekte	52
3. Symbole von Lotus Protector Manager	2	21. Ergebnisse des Sender Policy Frameworks	54
4. Statusleuchtanzeigen auf der Startseite	3	22. Typen von Response-Objekten	57
5. Kategorien für den Schutzstatus	3	23. Typen von Nachrichtenspeichern	64
6. Einstellungen für den Bewertungsstatus	4	24. Einstellungen für den Spamdatenfluss	71
7. Einstellungen für den Verkehrstatus	5	25. DNSBL-Listeneinstellungen	71
8. Einstellungen für den Ressourcenstatus	5	26. Einstellungen für Endbenutzerschnittstelle	72
9. Einstellungen für den Status der Updates	6	27. Vordefinierte Berichte	81
10. Einstellungen für den Systemstatus	7	28. Status von Komponenten und Lizenzen	89
11. Lizenzschlüsseleinstellungen	8	29. Tasks der Endbenutzerschnittstelle	97
12. Erforderliche Netzservices.	10	30. Allgemeine erweiterte Parameter	109
13. Lotus Protector for Mail Security-Kennwörter	12	31. Erweiterte Parameter für LDAP-Server	110
14. Beispiel für eine Routing-Tabelle	16	32. Erweiterte Parameter für Nachrichtenspeicher	111
15. Beispiel für die Konfiguration von DNS-MX-Einträgen mit Failover und Lastverteilung	19	33. Erweiterte Parameter für SMTP-Einstellungen	112
16. DNSBL-Grenz-IP-Adressen	29	34. Erweiterte Parameter für die DNSBL-Einstellungen	113
17. Bestandteile einer Richtlinienregel	47	35. Erweiterte Parameter für Clusterreplikation	113
18. Typen von Who-Objekten	49	36. Endbenutzerschnittstelle, erweiterte Parameter	114

Informationen zu dieser Veröffentlichung

Diese Veröffentlichung beschreibt die Funktionen und Fähigkeiten von IBM® Lotus® Protector for Mail Security.

Zielgruppe

Diese Veröffentlichung ist für Netzsystemadministratoren konzipiert, die für die Installation und Konfiguration von Lotus Protector for Mail Security verantwortlich sind. Dabei wenden sie die bewährten Verfahren der Mail Security an, konfigurieren SMTP-Services und führen bei Bedarf Anwendungen auf VMware aus.

Aktuelle Produktdokumentation

Die aktuelle Produktdokumentation finden Sie auf der IBM Lotus® Protector for Mail Security-Dokumentations-Website unter <https://www.ibm.com/developerworks/lotus/documentation/protector/mailsecurity/>.

Lizenzvereinbarung

Lizenzinformationen zu IBM Lotus® Protector for Mail Security finden Sie auf der IBM Website zu Lizenzvereinbarungen unter <http://www.ibm.com/software/sla/sladb.nsf/search>.

Neuigkeiten in Version 2.8

In der folgenden Tabelle werden neue Funktionen in IBM Lotus® Protector for Mail Security V2.8 aufgelistet und die ersten Schritte mit diesen Funktionen erläutert.

Tabelle 1. Neue Funktionen für Lotus Protector for Mail Security V2.8

Neue Funktion	Verwendungsweise
Analyse des Dateianhangs	Sie können Lotus Protector for Mail Security zum Überprüfen des Inhalts (Schlüsselwörter, reguläre Ausdrücke, URLs) einrichten, der eingehenden E-Mail-Nachrichten angehängt wurde. LMI-Navigation: SMTP > Analyse des Dateianhangs Weitere Informationen: „Inhalte der Dateien überprüfen, die eingehenden E-Mail-Nachrichten angehängt sind“ auf Seite 70
Globale IP-Zugriffsliste	Sie können eine Liste von IP-Adressen einrichten, denen der Zugriff beim Start einer eingehenden SMTP-Verbindung erlaubt oder verweigert wird. Diese Funktion wird vom dynamischen Hostreputationsfilter und den DNSBL-Einstellungen verwendet. LMI-Navigation: SMTP > SMTP-Konfiguration > Empfangender SMTP > Globale IP-Zugriffsliste Weitere Informationen: „Globale IP-Zugriffsliste konfigurieren“ auf Seite 28

Tabelle 1. Neue Funktionen für Lotus Protector for Mail Security V2.8 (Forts.)

Neue Funktion	Verwendungsweise
ICAP-Server	Sie können Lotus Protector for Mail Security so konfigurieren, dass für mit ICAP kompatible Clients, wie z. B. IBM® Connections, IBM Lotus Quickr® und Squid 3.x, Virenservices in Echtzeit bereitgestellt werden. LMI-Navigation: System > ICAP-Server Weitere Informationen: „ICAP-kompatible Clients Virenservices in Echtzeit bereitstellen“ auf Seite 14
Handhabung von Verweigerung für IP-Adressen mithilfe der Option "Ohne Hinweis löschen"	Sie können den SMTP-Service einrichten, um eine eingehende E-Mail-Nachricht abzulehnen, ohne den Absender der E-Mail darüber zu informieren, dass die E-Mail-Nachricht abgelehnt wurde. Mit dieser Methode wird verhindert, dass gültige E-Mail-Adressen von Spammern durchsucht werden. Diese Funktion wird vom dynamischen Hostreputationsfilter, der globalen IP-Zugriffsliste, der Empfängerüberprüfung und der Analyse der Nullebene (Zero Level Analysis, ZLA) verwendet.
Systemrouten manuell konfigurieren	Sie können die Option Netzwerkrouuten mithilfe von Verwaltungsschnittstellen verwalten verwenden, um zu beeinflussen, auf welche Weise Systemrouten durch die Routingrichtlinie behandelt werden. Wenn Sie die Option aktivieren, verwendet Lotus Protector for Mail Security die Systemrouten, die Sie in der lokalen Verwaltungsschnittstelle (LMI) konfiguriert haben. Wenn Sie diese Option inaktivieren, bleiben alle Routen unverändert, damit Sie spezielle Routingeinstellungen implementieren können, die in der lokalen Verwaltungsschnittstelle derzeit nicht verfügbar sind. LMI-Navigation: System > Routen Weitere Informationen: „Systemrouting manuell konfigurieren“ auf Seite 17
Aktualisierte Version von SUSE Linux Enterprise Server (V2.8.1.0)	Das zugrunde liegende Betriebssystem wird von SUSE Linux Enterprise Server 10 auf SUSE Linux Enterprise Server 11 aktualisiert.
Signaturen zum Abwehren von Angriffen von außen werden nicht mehr unterstützt	Diese Funktion ist nicht mehr verfügbar.

Technische Unterstützung

IBM stellt technische Unterstützung für berechtigte Kunden bereit.

Das IBM Unterstützungsportal

Bevor Sie sich bezüglich eines Problems an IBM wenden, besuchen Sie das IBM Unterstützungsportal unter <http://www.ibm.com/software/support>.

Die Anleitung für IBM Softwareunterstützung

Wenn Sie sich an die technische Unterstützung wenden müssen, verwenden Sie die Methoden, die in der Anleitung für IBM Softwareunterstützung unter <http://www14.software.ibm.com/webapp/set2/sas/f/handbook/home.html> erläutert werden.

Die Anleitung stellt die folgenden Informationen bereit:

- Registrierungs- und Berechtigungsanforderungen für die Unterstützung
- Telefonnummern der Kundenunterstützung für das Land, in dem Sie leben
- Informationen, die Sie vor dem Anruf bereithalten müssen

Lotus Protector for Mail Security Mit einer Befehlszeile verwenden

Die Verwendung der Befehlszeile für schreibgeschützten Zugriff (zum Anzeigen von Einstellungen, Services, Protokollen, Prozessen, Speicherplatz oder zum Abfragen der Datenbank) wird unterstützt. Die Befehlszeile zum Ausführen von Konfigurationsänderungen von Lotus Protector for Mail Security hebt Ihre IBM Support-Vereinbarung auf, sofern diese Prozeduren befolgt werden.

Änderungen, die mithilfe der Befehlszeile an Lotus Protector for Mail Security vorgenommen werden, müssen:

- Schriftlich von IBM Support autorisiert werden.
- Von einem IBM Partner, Wiederverkäufer oder internen Mitarbeiter implementiert werden.
- In einer Textdatei in `/root/lib/customization` auf der Lotus Protector for Mail Security-Verwaltungskonsolle zusammengefasst und verwaltet werden.

Die Änderungen, die Sie über die Befehlszeile an Lotus Protector for Mail Security vorgenommen haben, können mit zukünftigen Produktausgaben inkompatibel sein. Bei der Behebung neuer Probleme mit Lotus Protector for Mail Security könnten Sie IBM Support dazu aufgefordert werden, benutzerdefinierte Konfigurationen von Lotus Protector for Mail Security in eine Standardeinstellung zurückzusetzen.

Kapitel 1. Erste Schritte mit Lotus Protector Manager

In diesem Kapitel werden die ersten Schritte für die Verwendung von Lotus Protector for Mail Security beschrieben, nachdem Sie mit dem Konfigurationsassistenten die ersten Netzeinstellungen konfiguriert haben.

Im Lotus Protector Manager navigieren

In diesem Abschnitt werden die Navigationsfunktionen von Lotus Protector Manager erläutert.

Linkes Navigationsfenster

Wählen Sie im Fenster auf der linken Seite die Kategorie in der Baumstruktur aus, die Sie konfigurieren möchten. Einige Kategorien weisen mehrere Komponenten auf, die Sie konfigurieren können. Erweitern Sie die Baumstruktur, um eine Liste der Elemente anzuzeigen, die Sie konfigurieren können.

In der folgenden Tabelle werden die einzelnen Kategorien der Navigationsstruktur beschrieben:

Tabelle 2. Kategorien der Navigationsstruktur

Kategorie	Beschreibung
Homepage	Auf dieser Site werden Informationen zum aktuellen Allgemeinzustand und Systemstatus von Lotus Protector for Mail Security angezeigt, einschließlich Statistikdaten zu E-Mail-Nachrichten und Datenfluss.
Mail Security	Anhand der Optionen in der Kategorie "Mail Security" wird erläutert, wie eine E-Mail-Sicherheitsrichtlinie mit einer Reihe von Regeln konfiguriert wird, die festlegen, wie ein- und ausgehender E-Mail-Datenverkehr von Lotus Protector for Mail Security untersucht und gefiltert werden soll.
SMTP	Anhand der Optionen in der Kategorie "SMTP" wird erläutert, wie die Einstellungen des SMTP-Service für Lotus Protector for Mail Security konfiguriert und wie die Warteschlangen für den SMTP-Server verwaltet werden.
System	Anhand der Optionen in der Kategorie "System" wird erläutert, wie Benachrichtigungen über Statusmeldungen eingerichtet werden, wie die Firewall-Einstellungen konfiguriert werden und wie die Konfigurationseinstellungen für Lotus Protector for Mail Security angepasst werden, beispielsweise die Netzwerkeinstellungen, Kennwörter oder die Einstellung für Datum und Uhrzeit.
Sicherung und Wiederherstellung	Anhand der Optionen in der Kategorie "Sicherung und Wiederherstellung" wird erläutert, wie Momentaufnahmen von Konfigurationseinstellungen verwaltet, wie umfassende Systemsicherungen erstellt und wie Protokolldateien gesichert werden, die von Lotus Protector for Mail Security generiert werden.
Updates	Anhand der Optionen in der Kategorie "Updates" wird erläutert, wie der Status der lizenzierten Sicherheitsmodule angezeigt und wie Lotus Protector for Mail Security für das Herunterladen und Installieren von Updates für die Sicherheitsmodule und die Firmware konfiguriert wird.
Support	Anhand der Optionen in der Kategorie "Support" wird erläutert, wie Kontaktinformationen angezeigt und wie Support-Datendateien für den technischen Support von IBM konfiguriert werden.

Symbole von Lotus Protector Manager

In der folgenden Tabelle werden die Symbole beschrieben, die auf den Seiten im Lotus Protector Manager angezeigt werden:

Tabelle 3. Symbole von Lotus Protector Manager

Sym- bol	Beschreibung
	Klicken Sie auf dieses Symbol, um der Liste ein Element hinzuzufügen.
	Klicken Sie auf dieses Symbol, um ein Element in der Liste zu bearbeiten.
	Klicken Sie auf dieses Symbol, um ein Element aus der Liste zu entfernen. Anmerkung: Wenn Sie auf dieses Symbol klicken, wird in einigen Fällen eine Warnung angezeigt, weil das Element bereits anderweitig verwendet wird (z. B. in einer Richtlinienregel oder von einem anderen Objekt). Lösen Sie dann zunächst die Abhängigkeit auf, bevor Sie das Objekt entfernen.
	Wählen Sie ein Element in der Liste aus und klicken Sie auf dieses Symbol, um das Element in der Liste nach oben zu verschieben.
	Wählen Sie ein Element in der Liste aus und klicken Sie auf dieses Symbol, um das Element in der Liste nach unten zu verschieben.
	Wählen Sie ein Element in der Liste aus und klicken Sie auf dieses Symbol, um das Element in die Zwischenablage zu kopieren. Tipp: Sie können die Standardmethoden Umschalttaste+Klick oder Steuerungstaste+Klick verwenden, um benachbarte oder nicht benachbarte Elemente in der Liste auszuwählen.
	Klicken Sie auf dieses Symbol, um ein kopiertes Element von der Zwischenablage in eine Liste einzufügen. Eingefügte Elemente werden am Ende der Liste angezeigt.
	Wenn dieses Symbol auf einer Seite oder neben einem Feld auf einer Seite angezeigt wird, müssen Sie die erforderlichen Daten in einem Feld eingeben oder die eingegebenen Daten in einem Feld sind ungültig.

Administratorsitzung oder Modus mit eingeschränktem Zugriff

Nur jeweils ein Benutzer kann unbeschränkten Zugriff auf Lotus Protector Manager haben. Andere Benutzer können nur den Modus mit eingeschränktem Zugriff verwenden, der es ihnen ermöglicht, die aktuelle Konfiguration von Lotus Protector for Mail Security anzuzeigen, nicht jedoch, sie zu bearbeiten. Im Modus mit beschränktem Zugriff können Benutzer E-Mail-Nachrichten im Nachrichtenspeicher durchsuchen und anzeigen, Benutzer verwalten, Berichte abrufen und Protokolldateien anzeigen.

Wenn Sie sich bei Lotus Protector for Mail Security im Administratormodus anmelden möchten und bereits ein anderer Benutzer mit diesem Modus angemeldet ist, werden Sie aufgefordert, sich im Modus mit eingeschränktem Zugriff anzumelden oder die Verbindung des anderen Benutzers zu trennen, um eine Anmeldung im Administratormodus zu ermöglichen.

Startseite

Auf dieser Site werden Informationen zum aktuellen Allgemeinzustand und Systemstatus von Lotus Protector for Mail Security angezeigt, einschließlich Statistikdaten zu E-Mail-Nachrichten und Datenfluss.

Statusleuchtanzeigen

Die Statusleuchtanzeigen auf jeder Statusregisterkarte stellen eine kurze Statuszusammenfassung für Lotus Protector for Mail Security bereit:

Tabelle 4. Statusleuchtanzeigen auf der Startseite

Leuchtanzeige	Farbe	Beschreibung
 [G] Gut	Grün	Zeigt an, dass die Lotus Protector for Mail Security Services erwartungsgemäß ausgeführt werden.
 [W] Warnung	Gelb	Zeigt an, dass in einem oder mehreren Services für Lotus Protector for Mail Security ein Fehler aufgetreten ist. Korrigieren Sie diesen Fehler so bald wie möglich.
 [E] Fehler	Rot	Zeigt an, dass in einem oder mehreren Services für Lotus Protector for Mail Security ein Problem besteht. Lösen Sie dieses Problem umgehend. Tipp: Die Anzeige hält möglicherweise eine Erläuterung des Problems bereit sowie vorgeschlagene Aktionen zur Fehlerbehebung.

Schutzstatus

Die Statusregisterkarte **Schutz** gibt einen allgemeinen Überblick über die Kategorien von E-Mail-Nachrichten, die von Lotus Protector for Mail Security in einem bestimmten Zeitraum analysiert wurden. Zudem erfahren Sie auf dieser Seite, ob die von Lotus Protector for Mail Security bereitgestellte Schutzstufe nicht ausreichend ist (z.B. bei deaktivierter Firewall) und erhalten Vorschläge zur Behebung solcher Probleme.

Tabelle 5. Kategorien für den Schutzstatus

Kategorie	Beschreibung
Konformität	E-Mail-Nachrichten, die möglicherweise vertrauliche Daten enthalten
Erwünschte E-Mail	E-Mail-Nachrichten, die keine Werbung oder unerwünschten Inhalt enthalten.
Blockierung der IP-Adresse	E-Mail-Nachrichten, die durch den SMTP-Service zurückgewiesen wurden, da die IP-Adresse des sendenden Hosts als Spamming-Host bekannt ist
Weitere	E-Mail-Nachrichten, die keiner der anderen vordefinierten Kategorien zugeordnet werden können
Phishing	E-Mail-Nachrichten, die wie reguläre E-Mails aussehen, die jedoch in betrügerischer Absicht gesendet werden, um persönliche Informationen und Finanzdaten der Empfänger abzurufen
Empfängerüberprüfung	E-Mail-Nachrichten, die möglicherweise an einen Benutzer gesendet wurden, der nicht im Unternehmen vorhanden ist
Malware-Fernererkennung	E-Mail-Nachrichten, bei denen die Antivirensoftware bekannte Malwaredateien entdeckt hat, beispielsweise Computerviren, Computerwürmer, Trojanische Pferde, Rootkits oder Spyware (Programme, die ohne Berechtigung Informationen über einen Computer erfassen).
Virensignaturerkennung	E-Mail-Nachrichten, in denen die Antivirensoftware signaturbasierte Viren gefunden hat.
Spam	E-Mail-Nachrichten, die nicht angeforderte Werbung oder anstößige Inhalte enthalten
ZLA NDR	E-Mail-Nachrichten, die von dem ZLA-Analysemodul gefunden wurden. Die Übertragung dieser Nachrichten ist fehlgeschlagen. Sie haben den vorgesehenen Empfänger nicht erreicht.

Tabelle 5. Kategorien für den Schutzstatus (Forts.)

Kategorie	Beschreibung
ZLA Spam	E-Mail-Nachrichten, die von dem ZLA-Analysemodul gefunden wurden. Diese Nachrichten werden als unerwartete Massen-E-Mail-Nachrichten klassifiziert, wie Phishing, Werbung oder Malware.

Bewertungsstatus

Die Registerkarte **Bewertungsstatus** bietet einen Überblick über den aktuellen Allgemeinzustand von Lotus Protector for Mail Security.

Anmerkung: Lotus Protector for Mail Security kann die Verarbeitung des E-Mail-Datenverkehrs drosseln, um die Situation zu entschärfen (z. B. weniger eingehende E-Mail-Nachrichten von anderen Hosts akzeptieren), wenn einer der folgenden Werte zu hoch ist. Wenn Lotus Protector for Mail Security jedoch über einen langen Zeitraum eine Überlastung aufweist, sollten Sie eine Anpassung Ihrer Konfiguration erwägen.

Tabelle 6. Einstellungen für den Bewertungsstatus

Einstellung	Beschreibung
Datenbankwarteschlange	Die Anzahl der Datensätze der analysierten E-Mail-Nachrichten, die noch nicht in der Datenbank gespeichert wurden
Länge der Analysewarteschlange	Die aktuelle Belegung der SMTP-Warteschlange zur temporären Speicherung von E-Mail-Nachrichten bis zur Analyse durch Lotus Protector for Mail Security (<i>Warteschlange "unchecked"</i>)
Ressourcennutzung	Der aktuelle Status von Arbeitsspeicher und Plattenbelegung von Lotus Protector for Mail Security. Gültige Werte sind: • 0 = Die verfügbare Menge an freiem Speicher und Plattenspeicher ist ausreichend. • 1 = Lotus Protector for Mail Security hat einen Speicher- oder Plattenspeicherengpass erkannt, der diesen Vorgang negativ beeinflussen kann. Überwachen Sie diese Situation und beheben Sie den Fehler bei Bedarf. • 2 = Lotus Protector for Mail Security hat fast keine verfügbaren Ressourcen mehr. Es wird empfohlen, unverzüglich Abhilfe zu schaffen. Anmerkung: Wenn Lotus Protector for Mail Security einen Ressourcenengpass erkannt hat, generiert es das Ereignis (<i>MSM_ResourceError</i>) auf der Ereignisseite (System > Ereignisse). Das Ereignis beinhaltet zusätzliche Informationen zum Problem.
Warteschlange für Nachrichtenverfolgung	Der aktuelle Füllstand der Warteschlange, die zum Speichern der Nachrichtenverfolgungsdaten in der Datenbank von Lotus Protector for Mail Security dient.
Länge der IPC-Warteschlange	Der aktuelle Füllstand des Kommunikationskanals zwischen dem SMTP-Service und der E-Mail-Sicherheit.
Länge der Sendewarteschlange	Die aktuelle Belegung der SMTP-Servicewarteschlange für ausgehende E-Mail-Nachrichten (<i>Warteschlange "send"</i>)

Datenverkehrsstatus

Die Registerkarte **Datenverkehrsstatus** zeigt den eingehenden und ausgehenden Netzverkehr in einem bestimmten Zeitraum an.

Tabelle 7. Einstellungen für den Verkehrstatus

Einstellung	Beschreibung
Eingehend (Minutendurchschnitt)	Die Gesamtzahl der empfangenen E-Mail-Nachrichten innerhalb eines bestimmten Zeitraums
Ausgehend (Minutendurchschnitt)	Die Gesamtzahl der zustellten E-Mail-Nachrichten innerhalb eines bestimmten Zeitraums
In Warteschlange für Analyse eingereiht	Zeigt die Anzahl der E-Mail-Nachrichten an, die sich im Wartezustand befinden, um von Lotus Protector for Mail Security analysiert zu werden
In Warteschlange für Zustellung eingereiht	Zeigt an, wie viele E-Mail-Nachrichten analysiert wurden und sich im Wartestatus für die Zustellung durch das SMTP-Modul befinden
In Warteschlange für erneute Zustellung eingereiht	Zeigt die Anzahl der E-Mail-Nachrichten an, für die ein Zustellversuch an den SMTP-Zielsever mit einem temporären Fehler fehlgeschlagen ist, z. B. weil der Host nicht erreichbar war Achtung: Wenn sich eine große Anzahl von E-Mail-Nachrichten in der Warteschlange für die erneute Zustellung befindet, kann dies auf ein permanentes Problem bei der Zustellung hindeuten (z. B. aufgrund eines Konfigurationsfehlers).

Ressourcenstatus

Die Registerkarte **Ressourcenstatus** zeigt Informationen über die von Lotus Protector for Mail Security belegten Systemressourcen an. Diese Informationen können nützlich sein, wenn Sie sich mit einem Problem an IBM Support wenden müssen.

Tabelle 8. Einstellungen für den Ressourcenstatus

Einstellung	Beschreibung
System	
CPU-Auslastung (Prozentsatz)	Überwacht die Prozessorressourcen, die auf der Benutzerebene von Prozessen und dem System-Kernel verwendet werden.
Systembelastung	Überwacht die Menge der vom System verrichteten Arbeit.
Speicherauslastung (MB)	Überwacht, wie viel des installierten Speichers frei ist.
Festplatten	
System (MB)	Überwacht die Größe des Plattenspeicherplatzes, der verwendet wird, um Lotus Protector for Mail Security auszuführen.
Datenspeicher (MB)	Überwacht die Menge der gespeicherten Daten auf dem System, das Lotus Protector for Mail Security ausführt.
Datenbank (MB)	Überwacht die Größe des für die Datenbank von Lotus Protector for Mail Security verwendeten Plattenspeicherplatzes.
Nachrichtenspeicher (MB)	Überwacht, wie viel Plattenspeicherplatz für die E-Mail-Nachrichtenspeicher verwendet wird

Status der Updates

Die Registerkarte **Status der Updates** zeigt den aktuellen Status der letzten Updates für Lotus Protector for Mail Security an.

Tabelle 9. Einstellungen für den Status der Updates

Komponente	Beschreibung
Firmware des Systems	Die letzte Version der Firmware-Version der Lotus Protector for Mail Security-Software.
Inhaltsfilterdatenbank (Web)	Die Version der derzeit von Lotus Protector for Mail Security verwendeten Mail Security-Datenbank. Diese Webversion der Inhaltsfilterdatenbank enthält URLs und die Klassifizierung von Webseiten.
Inhaltsfilterdatenbank (Mail)	Die Version der derzeit von Lotus Protector for Mail Security verwendeten Mail Security-Datenbank. Die Mail-Version der Inhaltsfilterdatenbank enthält Spamsignaturen aller bekannten Spams (zusammengestellt von Spam-Collectors und weiteren Quellen).
Bayes-Filter-Datenbank	Die Version der derzeit von Lotus Protector for Mail Security verwendeten Bayes-Filter-Datenbank. Die Bayes-Filterdatenbank ist von IBM vortrainiert, um Spamnachrichten anhand bestimmter Wörter und anderer Tokens identifizieren zu können, die üblicherweise in regulären E-Mail-Datenströmen vorkommen.
Spamheuristik	Die Version der derzeit von Lotus Protector for Mail Security verwendeten Spamheuristiksignaturen. Spamheuristiksignaturen verwenden Regeln, die die Merkmale von Spamnachrichten beschreiben, um eingehende E-Mail-Nachrichten (Header und Haupttext) und Anhänge zu bewerten.
Spamschlüsselwortanalyse	Die Version der derzeit von Lotus Protector for Mail Security verwendeten Signaturen der Spamschlüsselwortanalyse. Die Signaturen der Spamschlüsselwortanalyse berücksichtigen Standardschlüsselwörter und -muster (reguläre Ausdrücke), die in Spam-E-Mail-Nachrichten üblicherweise gefunden werden.
Phishing	Die Version der derzeit von Lotus Protector for Mail Security verwendeten Phishingsignaturen. IBM verwendet eine Vielzahl an Methoden zur Erkennung von Phishing-E-Mail-Nachrichten. Das URL-Prüfprogramm kann Links auf Banking- und andere kommerzielle Sites in Spamnachrichten erkennen, die aus den Spam-Collectors kommen. Phishing-E-Mail-Nachrichten weisen außerdem im Vergleich zu anderen Spamnachrichten eine typische Heuristik auf. Sie werden in der Filterdatenbank gesondert kategorisiert.
CAL-Scripting	Ein Modul, das hoch spezialisierte Algorithmen zum Erkennen bestimmter Spamtypen enthält. Anmerkung: Dieses Modul wird von IBM verwaltet und aktualisiert.

Tabelle 9. Einstellungen für den Status der Updates (Forts.)

Komponente	Beschreibung
Antivirensignaturen	Die Version der derzeit von Lotus Protector for Mail Security verwendeten Antivirensignaturen. Die Antivirensignaturen enthalten eine von IBM definierte Liste von Virendefinitionen für bekannte Viren. Lotus Protector for Mail Security durchsucht den E-Mail-Datenverkehr nach diesen Signaturen und führt entsprechende Aktionen aus, um infizierte Dateien unter Quarantäne zu stellen.

Systemstatus

Die Registerkarte **Systemstatus** zeigt den aktuellen Status von Lotus Protector for Mail Security an.

Tabelle 10. Einstellungen für den Systemstatus

Einstellung	Beschreibung
Basisimage-Überarbeitung	Die Basisversion oder ursprüngliche Version der Lotus Protector for Mail Security-Software. Anmerkung: Die Basisversion ist die Softwareversion, die mit Lotus Protector for Mail Security geliefert wird bzw. die Softwareversion der aktuellsten Systemsicherung.
Firmware	Die derzeit installierte Firmware-Version der Lotus Protector for Mail Security-Software.
Betriebszeit	Die Zeit, die Lotus Protector for Mail Security bisher online war.
Letzter Neustart	Das Datum, an dem Lotus Protector for Mail Security eingeschaltet oder neu gestartet wurde, angezeigt im Format jjjj-mm-tt hh:mm:ss (z. B. 2011-12-31 12:45:10).
Systemzeit	Die aktuelle Systemzeit des Systems, auf dem die Lotus Protector for Mail Security-Software ausgeführt wird.
Gesamtzahl der Netzschnittstellen	Die Anzahl der physisch installierten Netzschnittstellen auf Lotus Protector for Mail Security.
Gebundene IP-Adressen	Die IP-Adressen, die derzeit von Lotus Protector for Mail Security wie vom Administrator konfiguriert verwendet werden.
Letzte Systemsicherung	Das Datum, an dem die letzte Systemsicherung erstellt wurde, angezeigt im Format yyyy-mm-dd hh:mm:ss (z. B. 2011-12-31 12:45:10).
Inhaltsanalyse-Bibliothek	Zeigt die derzeit für die Content Analysis Library (CAL) installierten Module an. Diese ermitteln die Kategorien der E-Mail-Nachrichten, die von Lotus Protector for Mail Security verarbeitet werden.

Abschnitt A: Empfohlene Tasks

Im Anschluss an die Installation und die Erstkonfiguration von Lotus Protector for Mail Security sollten Sie die in diesem Abschnitt aufgeführten Prozeduren ausführen.

Lizenzschlüssel installieren

Die Seite **Updates und Lizenzierung** (**Updates > Updates und Lizenzierung**) enthält wichtige Informationen zum aktuellen Status Ihrer Lizenzschlüssel, einschließlich Ablaufdaten.

Informationen zu diesem Vorgang

Sie können Informationen zu jeder Lizenz von Lotus Protector for Mail Security anzeigen, die Sie erwerben:

Tabelle 11. Lizenzschlüsseleinstellungen

Einstellung	Beschreibung
Seriennummer	Die Seriennummer des Lizenzschlüssels. Anmerkung: Jeder Lizenzschlüssel verfügt über eine eigene für Identität und OCN eindeutige Seriennummer.
OCN	Die Order Confirmation Number (OCN) oder Ihre Kundennummer bei IBM.
Ablauf	Das Datum, an dem die Lizenz abläuft, angegeben im Format jjjj-mm-tt: 2011-12-31.
Ablauf des Wartungsvertrags	Das Datum, an dem die Wartungsvereinbarung abläuft, angegeben im Format jjjj-mm-tt: 2011-12-31.

Vorgehensweise

1. Klicken Sie im Navigationsfenster auf **Updates > Updates und Lizenzierung**.
2. Klicken Sie auf die Registerkarte **Lizenzierung**.
3. Klicken Sie auf **Einen neuen Lizenzschlüssel installieren**.
4. Suchen Sie den Lizenzschlüssel oder stellen Sie diesen zur Verfügung.
5. Klicken Sie auf **Schlüssel installieren**. Lotus Protector for Mail Security installiert die Datei mit dem Lizenzschlüssel in einem geeigneten Verzeichnis.

Konfigurationseinstellungen sichern

Durch das Update von Lotus Protector for Mail Security wird sichergestellt, dass Ihr Produkt stets auf dem neuesten Stand ist. Vor der Installation von Updates, die sich auf die ursprünglichen Konfigurationseinstellungen auswirken können, wird Ihr System gesichert.

Informationen zu diesem Vorgang

Erstellen Sie eine Momentaufnahme der ursprünglichen Konfigurationseinstellungen für Lotus Protector for Mail Security, bevor Sie Firmware-Updates oder Änderungen an den Konfigurationseinstellungen vornehmen. Sie können später zusätzliche Momentaufnahme erstellen, wenn Sie andere Konfigurationseinstellungen verwenden oder neue Richtlinieneinstellungen testen möchten.

Die Datei `factoryDefault.settings` enthält standardmäßig die ursprünglichen Konfigurationseinstellungen von Lotus Protector for Mail Security. Erstellen Sie möglichst immer eine Momentaufnahme, bevor Sie Ihre Konfigurationseinstellungen ändern.

Vorgehensweise

1. Klicken Sie im Navigationsfenster auf **Sicherung und Wiederherstellung > System**.
2. Klicken Sie auf **Konfigurationssicherung verwalten**.
3. Wählen Sie im Abschnitt **Konfigurationssicherungen** eine Option aus:

Option	Bezeichnung
Momentaufnahme erstellen	1. Klicken Sie auf Neu. 2. Geben Sie einen Namen für die Momentaufnahme ein und klicken Sie auf Erstellen.
Momentaufnahme wiederherstellen	Wählen Sie die Momentaufnahme aus, die Sie wiederherstellen möchten, und klicken Sie auf Wiederherstellen .
Momentaufnahme löschen	Wählen Sie die Momentaufnahme aus, die Sie löschen möchten, und klicken Sie auf Löschen .
Momentaufnahme hochladen	1. Klicken Sie auf Neu. 2. Geben Sie den Namen der Momentaufnahme ein, die Sie hochladen möchten, und klicken Sie auf Hochladen.
Momentaufnahme herunterladen	Wählen Sie die Momentaufnahme aus, die Sie herunterladen möchten, und klicken Sie auf Herunterladen .

Updates für E-Mail-Sicherheit ausführen

Bevor Sie Lotus Protector for Mail Security verwenden, sollten Sie die neuesten Updates für die E-Mail-Sicherheit in die Datenbank herunterladen. Sie können Lotus Protector for Mail Security so konfigurieren, dass automatisch Updates vom IBM Download Center bezogen werden.

Informationen zu diesem Vorgang

Die Updates für E-Mail-Sicherheit bieten tägliche Updates von URLs und Spamsignaturen für Lotus Protector for Mail Security.

Wichtig: Damit die lokale E-Mail-Sicherheitsdatenbank aktuell bleibt, wird empfohlen, mindestens einmal täglich ein Update durchzuführen.

Vorgehensweise

1. Klicken Sie im Navigationsfenster auf **Updates > Updates und Lizenzierung**.
2. Klicken Sie auf die Option **Versionen online anzeigen** im unteren Bereich der Seite, um auf eine Liste für jedes Update und die entsprechenden Inhalte zuzugreifen.
3. Klicken Sie nach dem Herunterladen und Installieren Ihrer Lizenzschlüssel auf **Automatische Updates konfigurieren**.
4. Stellen Sie sicher, dass **E-Mail-Sicherheitsdatenbank automatisch aktualisieren** im Abschnitt **Updates der E-Mail-Sicherheitsdatenbank** aktiviert ist.
5. Klicken Sie auf **Änderungen speichern**.

Lokale Firewall konfigurieren

Möglicherweise müssen Sie die lokale Firewall für Lotus Protector for Mail Security konfigurieren, um den Zugriff auf die zur Verfügung gestellten Services über Netze zu steuern, die einer bestimmten Netzschnittstelle zugeordnet sind.

Informationen zu diesem Vorgang

Mit den Optionen auf dieser Seite können Sie den Zugriff auf Services steuern, die von Lotus Protector for Mail Security zur Verfügung gestellt werden. Damit Lotus Protector for Mail Security ordnungsgemäß ausgeführt werden kann, müssen Sie möglicherweise die Einstellungen für Ihre unternehmensweite Firewall oder für andere Firewalls ändern, die zwischen Lotus Protector for Mail Security und dem Serviceanbieter, z. B. einem Verzeichnisservice, implementiert sind.

Vorgehensweise

1. Klicken Sie im Navigationsfenster auf **System > Firewall**.
2. Stellen Sie sicher, dass die Services für Lotus Protector for Mail Security ordnungsgemäß aktiviert wurden und erreichbar sind:

Tabelle 12. Erforderliche Netzservices

Service	Portnummer	Beschreibung
SMTP	TCP 25	Ermöglicht den Zugriff auf den SMTP-Service über die angegebenen Netzschnittstellen, damit interne und externe SMTP-Server E-Mail-Nachrichten an Lotus Protector for Mail Security weiterleiten können
HTTPS	TCP 443	Ermöglicht den Zugriff auf Lotus Protector Manager aus Netzen, die den angegebenen Netzschnittstellen zugeordnet sind.
SSH	TCP 22	Ermöglicht es SSH-Clients (z. B. PuTTY), eine Verbindung mit der Befehlszeilenschnittstelle für Lotus Protector for Mail Security herzustellen.

Tabelle 12. Erforderliche Netzservices (Forts.)

Service	Portnummer	Beschreibung
Zugriff auf die Endbenutzer-.br schnittstelle	TCP 4443	Ermöglicht den Zugriff auf die Endbenutzerschnittstelle, mithilfe derer die Empfänger von E-Mail-Nachrichten unter Quarantäne gestellte E-Mail-Nachrichten aus Nachrichtenspeichern freigeben und Blockierlisten und Zulassungslisten verwalten können
SNMP	UDP 161	Ermöglicht den Zugriff auf den SNMP-Agenten von Lotus Protector for Mail Security, um Daten zum aktuellen Status mithilfe von SNMP-Get zu erfassen.
Datenbank-zugriff	TCP 5432	Ermöglicht den Clients eines Mail Security-Clusters den Zugriff auf die Datenbank des zentralen Systems. Achtung: Stellen Sie sicher, dass diese Option aktiviert ist, bevor Sie einen Mail Security-Cluster erstellen oder ein System mit einem Mail Security-Cluster verbinden.
Clusterkommunikation	TCP 4990	Ermöglicht den Mitgliedern eines Mail Security-Clusters die Kommunikation mit dem entsprechenden Host. Achtung: Stellen Sie sicher, dass diese Option aktiviert ist, bevor Sie einen Mail Security-Cluster erstellen oder ein System mit einem Mail Security-Cluster verbinden.
ICMP-Pingsignal		Ermöglicht es Lotus Protector for Mail Security, auf ICMP-Echoanforderungen (Pingbefehle) auf den angegebenen Netzschnittstellen zu antworten.

E-Mail-Adressen für Administratoren und von Accounts für Systembenachrichtigungen definieren

Sie müssen die E-Mail-Adressen für den Administrator Ihrer lokalen E-Mail-Umgebung sowie für die Definition der E-Mail-Konten einrichten, die von Lotus Protector Manager verwendet werden, um Statusbenachrichtigungen im Fall von unzustellbaren E-Mail-Nachrichten oder Quarantäneberichten zu versenden.

Vorgehensweise

1. Klicken Sie im Navigationsfenster auf **SMTP > Konfiguration**.
2. Klicken Sie auf die Registerkarte **Global**.
3. Stellen Sie folgende Informationen bereit:

Option	Bezeichnung
Rootdomäne	Die primäre Maildomäne des SMTP-Service. Dieser Wert wird z. B. vom SMTP-Service als Antwort auf den HELO/EHLO-Befehl gesendet.
Postmaster	Die E-Mail-Adresse der Person, die für das E-Mail-System im Unternehmen verantwortlich ist
Fehleradministrator	Die E-Mail-Adresse des Administrators, der bei permanenten Zustellungsproblemen benachrichtigt werden sollte Anmerkung: Wenn Sie dieses Feld freilassen, erhält nur der ursprüngliche Absender der E-Mail-Nachricht eine Benachrichtigung, wenn ein Zustellversuch für die E-Mail-Nachricht nicht erfolgreich war.

Option	Bezeichnung
Temporärer Fehleradministrator	Die E-Mail-Adresse des Administrators, der bei temporären Zustellungsproblemen benachrichtigt werden sollte Anmerkung: Wenn Sie dieses Feld freilassen, erhält nur der ursprüngliche Absender der E-Mail-Nachricht eine Benachrichtigung, wenn ein Zustellversuch für die E-Mail-Nachricht nicht erfolgreich war.
Neue E-Mail senden als	Die E-Mail-Adresse, die Lotus Protector Manager als Absender für lokal generierte E-Mail-Nachrichten verwendet
Quarantänebericht senden als	Die E-Mail-Adresse, die Lotus Protector Manager als Absender des Quarantäneberichts verwendet

4. Klicken Sie auf **Änderungen speichern**.

Abschnitt B: Optionale Tasks

Im Anschluss an die Installation und die Erstkonfiguration von Lotus Protector for Mail Security können Sie die in diesem Abschnitt aufgeführten optionalen Prozeduren ausführen.

Kennwörter für Lotus Protector for Mail Security ändern

Dieser Abschnitt beschreibt die Vorgehensweise bei der Änderung der Kennwörter für Lotus Protector for Mail Security-Accounts, die Sie oder ein anderer Administrator ursprünglich mithilfe des Konfigurationsassistenten eingerichtet haben.

Vorbereitende Schritte

Sie müssen das aktuelle Kennwort kennen, um ein Kennwort ändern zu können.

Informationen zu diesem Vorgang

Wenn Sie Lotus Protector for Mail Security konfigurieren, müssen Sie für diese Accounts Kennwörter eingeben:

Tabelle 13. Lotus Protector for Mail Security-Kennwörter

Account	Zweck
Root	Ermöglicht Ihnen den Zugriff auf das Betriebssystem von Lotus Protector for Mail Security.
Admin	Ermöglicht Ihnen den Zugriff auf den Konfigurationsassistent und auf den Lotus Protector Manager für den Lotus Protector for Mail Security.

Vorgehensweise

1. Klicken Sie im Navigationsfenster auf **System > Administratorkennwörter**.
2. Wählen Sie eine Option aus:

Wenn Sie Folgendes ändern möchten...	Dann...
Rootkennwort	1. Geben Sie im Abschnitt Root das aktuelle Kennwort ein. 2. Klicken Sie auf Kennwort eingeben. 3. Geben Sie das neue Kennwort ein und bestätigen Sie es.

Wenn Sie Folgendes ändern möchten...	Dann...
Administratorkennwort	1. Geben Sie im Abschnitt Admin das aktuelle Kennwort ein. 2. Klicken Sie auf Kennwort eingeben. 3. Geben Sie das neue Kennwort ein und bestätigen Sie es.

3. Klicken Sie auf **Änderungen speichern**.

Einstellungen für Datum und Zeit ändern

Dieser Abschnitt beschreibt die Vorgehensweise beim Ändern von Datum und Uhrzeit von Lotus Protector for Mail Security. Außerdem wird beschrieben, wie das Network Time Protocol (NTP) aktiviert wird, um die Uhrzeit von Lotus Protector for Mail Security mit einem Netzzeitserver zu synchronisieren.

Informationen zu diesem Vorgang

Die Seite **Uhrzeit** enthält immer die zuletzt manuell konfigurierten Werte der Datums- und Zeitoptionen und nicht das tatsächliche Datum und die tatsächliche Uhrzeit. Wenn Sie die Einstellungen speichern, wird Lotus Protector for Mail Security auf die aktuell konfigurierten Werte eingestellt, unabhängig davon, ob Sie diese geändert haben.

Wichtig: Aktualisieren Sie die Zeit und das Datum, bevor Sie die Einstellungen speichern, um ein Zurücksetzen dieser Werte auf die davor konfigurierten Werte zu vermeiden.

Vorgehensweise

1. Klicken Sie im Navigationsfenster auf **System > Uhrzeit**.
2. Wählen Sie eine Option aus:

Wenn Sie folgende Aktion ausführen möchten...	Dann...
Ändern Sie Datum und Uhrzeit von Lotus Protector for Mail Security	1. Klicken Sie auf den Pfeil Datum und Uhrzeit, um den Kalender anzuzeigen. 2. Wählen Sie den richtigen Monat und das richtige Datum aus. Tipp: Ändern Sie mithilfe der Pfeile oben den Monat und das Jahr im Kalender. 3. Wählen Sie in den Kontrollkästchen Uhrzeit die Stunde und die Minuten aus. 4. Klicken Sie in den Bereich außerhalb des Kalenders, um diesen zu schließen. 5. Klicken Sie auf den Pfeil Zeitzone und wählen Sie die Zeitzone Ihrer Region aus. 6. Klicken Sie auf Änderungen speichern.
Aktivieren Sie das Network Time Protocol (NTP).	Anmerkung: Das NTP synchronisiert die Konfigurationszeit mit einem Netzzeitserver. 1. Aktivieren Sie das Kontrollkästchen NTP aktivieren und geben Sie anschließend den Namen des NTP-Servers ein. 2. Klicken Sie auf Änderungen speichern.

Anmerkung: Wenn Sie eine Task planen, verwenden Sie einen absoluten Wert, um den Zeitpunkt der Ausführung festzulegen (beispielsweise planen Sie die Ausführung einer Task für den 2011-10-10 um 10:10).

Wenn die Zeit auf dem Lotus Protector for Mail Security-System geändert wird, kann dies Auswirkungen auf den Zeitpunkt haben, zu dem eine geplante Task ausgeführt wird. Wenn Sie die Systemzeit vorstellen, werden alle Tasks, die im Zeitrahmen zwischen dem alten und dem neuen Wert geplant sind, sofort ausgeführt. Wenn Sie die Systemzeit zurückstellen, werden alle geplanten Tasks verzögert. Wiederholt auftretende Tasks werden nicht ausgeführt, wenn Sie die Systemzeit auf einen Wert vorstellen, der außerhalb der konfigurierten Zeit liegt.

ICAP-kompatiblen Clients Virenservices in Echtzeit bereitstellen

In diesem Thema wird erläutert, auf welche Weise Lotus Protector for Mail Security aktiviert wird, um ICAP-kompatiblen Clients Virenservices in Echtzeit bereitzustellen wie beispielsweise IBM Connections, IBM Lotus Quickr oder Squid 3.x.

Informationen zu diesem Vorgang

Für spezielle Anleitungen zum Aktivieren von Virenservices für IBM Connections oder IBM Lotus Quickr besuchen Sie die IBM Connections-Wikisite unter <http://www.lotus.com/ldd/lcwiki.nsf> oder die IBM Lotus Quickr-Wikisite unter <http://www.lotus.com/ldd/lqwiki.nsf>.

Vorgehensweise

1. Klicken Sie im Navigationsfenster auf **System > ICAP-Server**.
2. Aktivieren Sie das Kontrollkästchen **ICAP-Server aktivieren**.
3. Geben Sie den Serverport für den ICAP-Server ein - normalerweise Port 1344.

Netzschnittstellen verwalten

Die Erstkonfiguration des Management-Ports, des Standard-Gateway-Ports sowie von DNS-Servern kann bei Bedarf geändert werden.

Warum kann eine Änderung der Netzeinstellungen erforderlich sein?

Änderungen der Netzeinstellungen können aus folgenden Gründen erforderlich sein:

- Änderungen der Netzrichtlinien Ihres Unternehmens
- Neustrukturierung Ihres Unternehmens
- Wechsel Ihres Internet-Service-Providers
- Änderung Ihrer Adressen
- Angabe von DHCP-Einstellungen
- Änderung von DNS-Einstellungen

Externe Schnittstellen konfigurieren

Sie können für die externen Schnittstellen einen DHCP-Server verwenden oder die IP-Adresse und DNS-Server für jede Netzschnittstelle manuell festlegen.

Vorgehensweise

1. Klicken Sie im Navigationsfenster auf **System > Netzwerk**.
2. Klicken Sie auf die Registerkarte **Externe Schnittstelle**.
3. Aktivieren Sie das Kontrollkästchen **Aktiviert**.
4. Geben Sie den Hostnamen von Lotus Protector for Mail Security in diesem Format ein:
appliance.example.com
5. Wählen Sie einen IP-Adresstyp aus:

Option	Bezeichnung
DHCP	1. Wählen Sie DHCP aus. 2. Wählen Sie bei Bedarf MAC-Klonen aktivieren und geben Sie anschließend 6 Hexadezimalpaare aus, die durch Doppelpunkte getrennt sind: AA:BB:CC:11:22:33
Statisch	1. Wählen Sie Statisch aus. 2. Geben Sie die IP-Adresse für die externe Schnittstelle von Lotus Protector for Mail Security ein und drücken Sie anschließend die EINGABETASTE. 3. Geben Sie den Wert der Subnetzmaske (Netzmaske) ein. 4. Geben Sie die IP-Adresse des Gateways ein.

6. Wählen Sie eine Einstellung für Ihren Domänennamensserver (DNS):

Option	Bezeichnung
Dynamische Einstellungen verwenden (aktiviert)	Aktiviert dynamische Einstellungen für Ihren Domänennamensserver. Tipp: Dynamische Einstellungen können Sie nur im Zusammenhang mit DHCP oder PPPoE verwenden. Sie können diese Einstellungen nicht verwenden, wenn Ihre externe Schnittstelle eine statische IP-Adresse verwendet.
Dynamische Einstellungen verwenden (deaktiviert)	Verwendet statische Einstellungen für Ihren Domänennamensserver: • Geben Sie die IP-Adresse für Primärer DNS-Server, Sekundärer DNS-Server, Tertiärer DNS-Server in Dezimalschreibweise mit Trennzeichen ein: 127.0.0.1

7. Klicken Sie auf **Änderungen speichern**.

Interne Schnittstellen konfigurieren

Sie können die Netzschnittstelle konfigurieren, die von Lotus Protector for Mail Security verwendet werden soll.

Vorgehensweise

1. Klicken Sie im Navigationsfenster auf **System > Netzwerk**.
2. Klicken Sie auf die Registerkarte **Interne Schnittstelle**.
3. Klicken Sie auf **Hinzufügen**.
4. Wählen Sie aus der Liste eine Schnittstelle aus.

Tipp: ETH0 ist immer die primäre interne Schnittstelle.

5. Aktivieren Sie das Kontrollkästchen **Aktiviert**.
6. Geben Sie die folgenden IP-Adressen oder Werte ein:
 - Ziel-IP-Adresse
 - Wert der Subnetzmaske
 - IP-Adresse des Gateways
7. Klicken Sie auf **Änderungen speichern**.

Netzübertragungen weiterleiten

Lotus Protector for Mail Security leitet Datenverkehr in verbundenen Netzen und Teilnetzen weiter. Dafür müssen der Schnittstelle IP-Netzeinstellungen einschließlich IP-Adressen, Subnetzmasken und IP-Adressen der Gateway-Router zugeordnet werden.

Weiterleiten von Datenverkehr durch Lotus Protector for Mail Security

Lotus Protector for Mail Security leitet Datenverkehr in verbundenen Netzen und Teilnetzen weiter. Dafür müssen der Schnittstelle IP-Netzeinstellungen einschließlich IP-Adressen, Subnetzmasken und IP-Adressen der Gateway-Router zugeordnet werden.

Im Route-Modus besteht eine der grundlegenden Funktionen von Lotus Protector for Mail Security darin, den Netzdatenverkehr von einem physischen Netz an ein anderes Netz weiterzuleiten. Diese Netze sind mit den verschiedenen Schnittstellen von Lotus Protector for Mail Security verbunden.

Damit eine Weiterleitung erfolgt, müssen Sie die Schnittstellen aktivieren und mit ihren entsprechenden Netzen physisch verbinden. Sie müssen den Schnittstellen auch Netzinformationen wie IP-Adressen und Subnetzmasken zuordnen. Die externen und internen Schnittstellen werden während der Erstkonfiguration aktiviert und konfiguriert. Bei Bedarf können Sie weitere interne Schnittstellen aktivieren, um Lotus Protector for Mail Security mit anderen internen Netzen zu verbinden.

Vorrangige Route in der Routing-Tabelle

Bei mindestens zwei Routen mit einem gleichen Ziel hat die spezifischere Route Vorrang in der Routing-Tabelle.

In diesem Beispiel verwendet ein für den Host 10.1.1.1 bestimmtes Paket die Route 192.168.1.2.

Tabelle 14. Beispiel für eine Routing-Tabelle

Ziel	Subnetzmaske	IP-Adresse des Gateways
10.0.0.0	255.0.0.0	192.168.1.1
10.1.1.0	255.255.255.0	192.168.1.2
10.1.0.0	255.255.0.0	192.168.1.3

Eine statische Route hinzufügen

Sie können Lotus Protector for Mail Security eine statische Route hinzufügen.

Vorgehensweise

1. Klicken Sie im Navigationsfenster auf **System > Routen**.
2. Klicken Sie auf das Symbol **Hinzufügen**.
3. Geben Sie die folgenden IP-Adressen oder Werte ein:
 - Ziel-IP-Adresse
 - Wert der Subnetzmaske
 - IP-Adresse des Gateways
4. Geben Sie bei Bedarf einen Wert im Feld **Metrik** ein.

Anmerkung: Die Metrik (oder Hopanzahl) gibt die Anzahl der Routen oder Segmente zwischen der Quelle und dem Ziel an.

5. Klicken Sie auf **OK** und anschließend auf **Änderungen speichern**.

Systemrouting manuell konfigurieren

In diesem Thema wird erläutert, auf welche Weise die Option **Netzwerkrouuten mithilfe von Verwaltungsschnittstellen verwalten** die Behandlung von Systemrouten durch die Routingrichtlinie beeinflusst.

Vorgehensweise

1. Klicken Sie im Navigationsfenster auf **System > Routen**.
2. Wählen Sie für die Option **Netzwerkrouuten mithilfe von Verwaltungsschnittstellen verwalten** eine der folgenden Optionen aus:

Option	Bezeichnung
Kontrollkästchen aktivieren	Alle Systemrouten werden gemäß der Konfiguration in der lokalen Verwaltungsschnittstelle eingerichtet. Anpassungen, die über die Befehlszeile vorgenommen wurden, werden überschrieben.
Aktivierung des Kontrollkästchens aufheben	Alle Systemrouteneinstellungen bleiben unverändert. Systemrouten werden weder gelöscht noch erstellt. Dieses Szenario funktioniert sehr gut in Verbindung mit Netzumgebungen, für die spezielle Netzeinstellungen erforderlich sind, die derzeit in der lokalen Verwaltungsschnittstelle nicht verfügbar sind. Beispiel: Sie möchten die Konsole verwenden, um RoutingEinstellungen hinzuzufügen, die in der lokalen Verwaltungsschnittstelle nicht verfügbar sind (/etc/sysconfig/network/routes). Lotus Protector for Mail Security erkennt die SystemroutingEinstellungen, die Sie hinzugefügt haben, ändert diese aber nicht.

3. Klicken Sie auf **Änderungen speichern**.

Kapitel 2. SMTP-Konfiguration

In diesem Kapitel wird beschrieben, wie Lotus Protector for Mail Security konfiguriert wird, um den E-Mail-Datenverkehr zu verarbeiten.

Lotus Protector for Mail Security implementieren

Der Administrator, der Lotus Protector for Mail Security einrichtet, muss sicherstellen, dass der gesamte eingehende SMTP-Datenverkehr über Lotus Protector for Mail Security weitergeleitet wird, bevor er an interne Mail-Server zugestellt wird.

In diesem Abschnitt werden die für den Internet-Mail-Austausch verwendeten Verfahren beschrieben. Außerdem erhalten Sie Informationen darüber, in welchem Zusammenhang diese Verfahren mit der Einrichtung von Lotus Protector for Mail Security stehen und wie sie diese beeinflussen. Sie sollten diese Informationen lesen, wenn Sie mit Implementierungen von Internet-Mail-Exchangern und deren Konfiguration nicht vertraut sind.

Direktaufruf: Wenn Sie lediglich Informationen darüber erhalten möchten, inwiefern MX-Einträge Ihr Setup von Lotus Protector for Mail Security beeinflussen, finden Sie in den Absätzen, die mit **Fast Path** gekennzeichnet sind, eine kurze Erläuterung des jeweiligen Abschnitts.

DNS-MX-Einträge

Wenn eine E-Mail-Nachricht über das Internet versendet wird, muss der Absender der E-Mail-Nachricht den Namen des empfangenden Hosts ermitteln, der für die Verarbeitung von E-Mail-Nachrichten für eine Domäne verantwortlich ist (die Domänenkomponente der E-Mail-Adresse, z. B. `ibm.com` in `joe@ibm.com`). Um den Namen des empfangenden Hosts zu ermitteln, fragt der Absender die Mail-Exchanger-Einträge (MX-Einträge) vom DNS-Server des Empfängers ab. Diese Einträge gehören zu der Domäne, die in der Domänenkomponente der E-Mail-Adresse des Empfängers gefunden wurde. Dieser Eintrag verweist normalerweise auf einen vollständig qualifizierten Hostnamen (beispielsweise `server1.ibm.com`), der in eine konkrete IP-Adresse (wird als *A-Eintrag* bezeichnet) aufgelöst wird.

MX-Einträge enthalten ein Attribut, das als *MX-Einstellung* bezeichnet wird. Eine MX-Einstellung wird vom Absender zur Ermittlung der Priorität eines Mail-Servers verwendet, wenn für eine einzelne Domäne mehrere Hosts zuständig sind. Standardmäßig wählt der sendende Host den Mail-Server mit dem kleinsten Wert der MX-Einstellung (der die geringsten Kosten angibt, ähnlich dem Messwert in IP-Routen) aus und wechselt zu einem anderen Host mit der geringsten Einstellung, auf den verwiesen wird. Wenn zwei oder mehr MX-Einträge den gleichen Einstellungswert haben, wählt der Absender möglicherweise einen Mail-Server nach dem Zufallsprinzip aus (je nach Implementierung des sendenden Servers). Identische Einstellungen für mehrere MX-Einträge werden im Allgemeinen verwendet, um die Last auf mehrere Server zu verteilen.

Tabelle 15. Beispiel für die Konfiguration von DNS-MX-Einträgen mit Failover und Lastverteilung

Zuständige Mail-Exchanger	MX-Einstellung
server1.ibm.com	10
server2.ibm.com	20
server3.ibm.com	20

Nehmen Sie beispielsweise an, dass die MX-Einträge für `ibm.com` mit den in Tabelle 15 aufgeführten Werten konfiguriert sind. Ein SMTP-Server versucht zuerst, eine E-Mail-Nachricht für `joe@ibm.com` an

server1.ibm.com zuzustellen. Wenn der sendende SMTP-Server keine Verbindung mit server1.ibm.com herstellen kann, wählt er nach dem Zufallsprinzip server2.ibm.com oder server3.ibm.com für die Zustellung der Nachricht aus.

Direktaufruf: Sendende SMTP-Server müssen Informationen darüber haben, wohin sie E-Mail-Nachrichten für Ihre Domänen zustellen sollen. Stellen Sie sicher, dass Sie für alle Ihre Domänen MX-Einträge eingerichtet haben. Abhängig von Ihrem Implementierungsszenario (Informationen finden Sie im Abschnitt zu eingehendem SMTP-Datenverkehr) sollten diese MX-Einträge auf einen Hostnamen (*A-Eintrag*) verweisen, der wiederum auf eine öffentliche IP-Adresse verweist, die sich im Besitz von Lotus Protector for Mail Security befindet.

Anmerkung: Das Füllen der DNS-Einträge kann im Internet bis zu drei Tage dauern. Wenn Sie DNS-Einträge für Ihre Umgebung ändern müssen, sollten Sie sicherstellen, dass Sie während dieser Zeit SMTP-Datenverkehr an veraltete IP-Adressen auf Lotus Protector for Mail Security umleiten können.

Eingehender SMTP-Datenverkehr

Wenn ein sendender Host versucht, eine E-Mail-Nachricht an einen SMTP-Zielserver zuzustellen, der durch DNS-MX-Einträge angegeben wird, versucht er, eine Verbindung mit dem Zielhost herzustellen. E-Mail-Nachrichten werden standardmäßig nicht immer direkt durch den sendenden Server an das entsprechende Ziel gesendet. Der sendende Server übermittelt die E-Mail-Nachricht stattdessen möglicherweise an einen anderen SMTP-Server, der dann für die Zustellung der E-Mail-Nachricht verantwortlich ist. Dieses Verfahren ist auch als *Weiterleiten* bekannt. Ein SMTP-Server, der das Weiterleiten ermöglicht, wird als *SMTP-Relay* bezeichnet.

Lotus Protector for Mail Security fungiert als SMTP-Relay, wenn sendende Hosts E-Mail-Nachrichten an Ihre Benutzer weiterleiten dürfen. Im Gegensatz zu anderen SMTP-Relays speichert Lotus Protector for Mail Security keine E-Mail-Nachrichten und leitet E-Mail-Nachrichten nicht an interne Mail-Server weiter. Stattdessen werden eingehende E-Mail-Nachrichten lokal gespeichert, bis diese analysiert und verarbeitet wurden. Nachdem eine E-Mail-Nachricht analysiert wurde, wird die Zustellung der E-Mail-Nachricht abhängig von Ihren Richtlinienregeln zugelassen oder abgelehnt. Wenn die Zustellung der E-Mail-Nachricht zugelassen wird, leitet Lotus Protector for Mail Security die E-Mail-Nachricht an interne SMTP-Server weiter, mit denen Benutzer eine Verbindung herstellen, um auf ihre E-Mail-Accounts zuzugreifen.

In den meisten Fällen wird Lotus Protector for Mail Security so implementiert, dass eingehende E-Mail-Nachrichten direkt aus dem Internet empfangen werden, d. h. der SMTP-Datenverkehr (auf der IP-Ebene) wird über ein Gateway oder eine Firewall an Lotus Protector for Mail Security weitergeleitet.



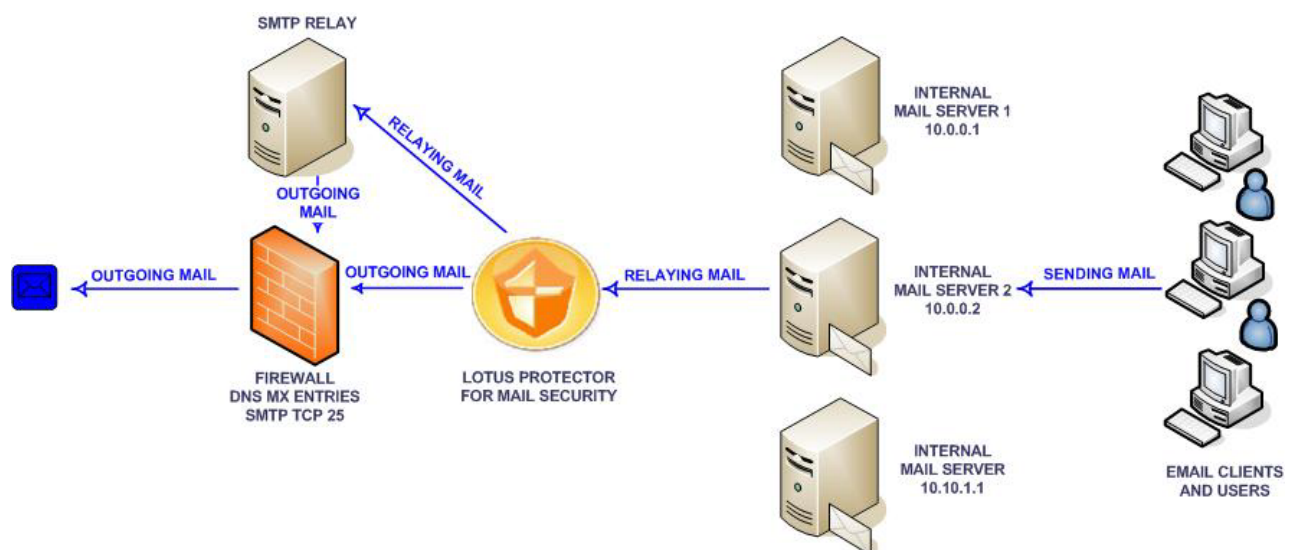
In manchen Szenarien kann es jedoch sinnvoll oder erforderlich sein, eingehende E-Mail-Nachrichten über andere SMTP-Server weiterzuleiten, bevor diese an Lotus Protector for Mail Security übergeben werden können (z. B. wenn Sie eine zusätzliche Analyse ausführen müssen, oder um hohe Systemauslastungen im E-Mail-Datenverkehr oder Netzeinschränkungen auszugleichen).

Direktaufruf: Stellen Sie im Hinblick auf die Implementierung sicher, dass alle E-Mail-Nachrichten aus dem Internet an Lotus Protector for Mail Security weitergeleitet werden können. Sie müssen möglicherweise Firewallregeln für den SMTP-Datenverkehr (standardmäßig für den TCP-Port 25) anpassen, geeignete Weiterleitungsregeln auf Ihren SMTP-Relays hinzufügen oder andere vorgeschaltete Einheiten neu konfigurieren.

Wichtig: Lotus Protector for Mail Security fungiert als SMTP-Relay. Datenströme in Ihrem Netz werden nicht analysiert und IP-Datenverkehr kann nicht weitergeleitet oder geroutet werden, da es sich hierbei nicht um ein Gateway handelt. E-Mail-Nachrichten müssen über Lotus Protector for Mail Security weitergeleitet werden. Eine integrierte Implementierung steht als Implementierungsoption für Lotus Protector for Mail Security nicht zur Verfügung.

Ausgehender SMTP-Datenverkehr

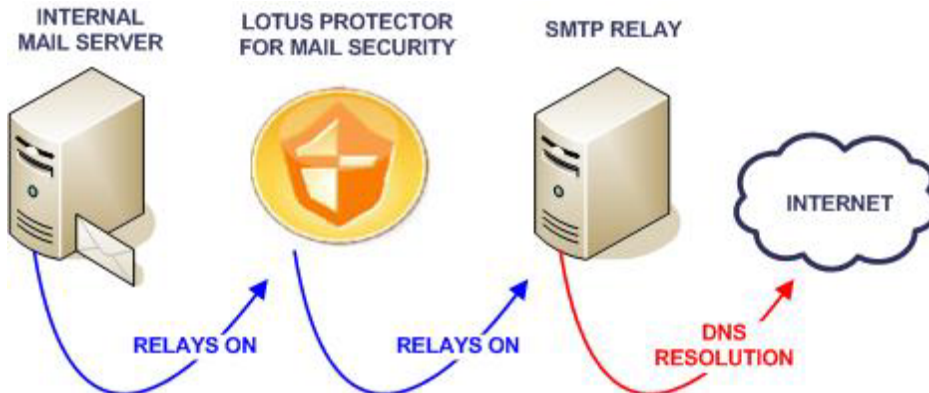
Sie können Lotus Protector for Mail Security auch verwenden, um ausgehenden SMTP-Datenverkehr zu verarbeiten. Dabei werden E-Mail-Nachrichten, die Ihre Umgebung verlassen, analysiert und weitergeleitet. Sie können Lotus Protector for Mail Security beispielsweise verwenden, um zu verhindern, dass E-Mail-Nachrichten mit vertraulichen Daten aus Ihrer Umgebung gesendet werden, um die verschlüsselte Zustellung von vertraulichen Daten zu erzwingen, um E-Mail-Nachrichten bei Netzeinschränkungen an andere SMTP-Server weiterzuleiten oder um Statistikdaten zum ausgehenden Datenverkehr zu erstellen.



Wie im Abschnitt zu DNS-MX-Einträgen erwähnt, müssen SMTP-Server ermitteln, wohin E-Mail-Nachrichten an eine bestimmte Domäne zugestellt werden sollen. Im Allgemeinen versuchen SMTP-Server, E-Mail-Nachrichten durch DNS-Auflösung und durch direkte Kommunikation mit einem der angegebenen Server zuzustellen.



Sie können SMTP-Server auch so konfigurieren, dass alle E-Mail-Nachrichten (oder nur eine Teilmenge der E-Mail-Nachrichten an die konfigurierten Domänen) an andere SMTP-Relays weitergeleitet werden, welche wiederum für die Zustellung dieser E-Mail-Nachrichten verantwortlich sind. Dieses Verhalten können Sie definieren, indem Sie der Konfiguration des SMTP-Servers Weiterleitungsregeln hinzufügen.



Direktaufruf: Wenn Sie Lotus Protector for Mail Security für die Weiterleitung ausgehender E-Mails einrichten möchten, müssen Sie Ihren internen Mail-Servern Weiterleitungsregeln hinzufügen, die es ihnen ermöglichen, ausgehende E-Mail-Nachrichten an Lotus Protector for Mail Security weiterzuleiten. Aufgrund der integrierten Überprüfung zur Verhinderung der Weiterleitung müssen Sie die internen Mail-Server als Relay-Hosts für Lotus Protector for Mail Security hinzufügen, damit Lotus Protector for Mail Security E-Mail-Nachrichten an jede Domäne von diesen Hosts akzeptiert. Wählen Sie aus, ob Lotus Protector for Mail Security E-Mail-Nachrichten direkt über DNS-Auflösung zustellen soll oder ob ausgehende E-Mail-Nachrichten an andere SMTP-Relay-Server weitergeleitet werden sollen, die wiederum die Zustellung übernehmen.

Anmerkung: Lotus Protector for Mail Security greift bei Domänen, für die es keine Weiterleitungsregel gibt, automatisch auf die DNS-Auflösung zurück.

Einstellungen für den SMTP-Service konfigurieren

Sie können das Verhalten des SMTP-Moduls von Lotus Protector for Mail Security konfigurieren. Ebenso können Sie konfigurieren, wohin E-Mail-Nachrichten, die von lokalen Domänen empfangen wurden, zugestellt werden sollen. Zusätzlich können Sie einige Filteroptionen auf der SMTP-Ebene einstellen.

Allgemeine Einstellungen für den SMTP-Service konfigurieren

Dieser Abschnitt beschreibt die Vorgehensweise bei der Konfiguration des Verhaltens für den SMTP-Service beim Empfangen von E-Mail-Nachrichten von anderen SMTP-Servern.

Vorgehensweise

1. Klicken Sie im Navigationsfenster auf **SMTP > Konfiguration**.
2. Klicken Sie auf die Registerkarte **Empfangender SMTP > Einstellungen**.
3. Stellen Sie folgende Informationen bereit:

Option	Bezeichnung
Protokollierung aktivieren	Weist den SMTP-Service an, Informationen zur Zustellung von E-Mail-Nachrichten in eine Protokolldatei zu schreiben. Diese Protokolldatei hat den Namen smtp-jjjjmmtt0000. Anmerkung: Der SMTP-Service erfasst in der Protokolldatei mehrere Zeilen zu jedem Zustellversuch. Bei erfolgreichen Zustellversuchen schreibt der SMTP-Service einen Protokolleintrag für jeden Empfänger einer E-Mail-Nachricht sowie einen weiteren Protokolleintrag, wenn die Übertragung der E-Mail-Nachricht erfolgreich war.
Port	Gibt die Portnummer an, auf der der SMTP-Service empfangsbereit ist. Standard: Port 25 Achtung: Wenn Sie diesen Wert ändern, können andere SMTP-Server möglicherweise keine E-Mail-Nachrichten an Lotus Protector for Mail Security übertragen, da diese Server versuchen, eine Verbindung mit dem SMTP-Standardport (TCP-Port 25) zu öffnen. Wenn Sie den Empfangsport des SMTP-Service ändern müssen, können Sie eine Konvertierungsregel für die Firewall hinzufügen.
Max. Anzahl Empfänger pro Nachricht	Ein SMTP-Server kann versuchen, eine E-Mail-Nachricht in einem einzigen Vorgang an mehrere Empfänger zu übertragen. Mit diesem Wert wird die maximal zulässige Anzahl von Empfängern für einen einzelnen Übertragungsvorgang festgelegt. Standard: 100 Empfänger
Max. Nachrichten pro Sitzung	Ein SMTP-Server kann versuchen, innerhalb einer Verbindung mehrere E-Mail-Nachrichten an Lotus Protector for Mail Security zu übermitteln. Dieser Wert gibt an, wie viele E-Mail-Nachrichten ein SMTP-Server übertragen darf, bevor eine neue Verbindung mit Lotus Protector for Mail Security hergestellt werden muss.

Option	Bezeichnung
Sitzungszeitlimit	Gibt die Zeitdauer an, nach der die SMTP-Sitzung abläuft. Eine Zeitlimitüberschreitung kann auftreten, wenn der SMTP-Service innerhalb des festgelegten Zeitrahmens keine Daten vom sendenden SMTP-Server erhält. In diesem Fall beendet der SMTP-Service die Verbindung mit dem Peer. Standard: 60 Sekunden
Max. Nachrichtengröße (KB)	Definiert die maximale Größe einer E-Mail-Nachricht (in Kilobyte), die der SMTP-Service von anderen SMTP-Servern annehmen kann Anmerkung: Wenn Sie diesen Wert auf null setzen, sind alle Nachrichtengrößen für den SMTP-Service zulässig.
NULL-Absender zulassen	Wenn diese Option aktiviert ist, nimmt der SMTP-Service E-Mail-Nachrichten auch dann an, wenn der sendende SMTP-Server keinen Absender im Befehl MAIL FROM: angegeben hat. Wenn deaktiviert, weist der SMTP-Service die Übertragung zurück.
Max. Anzahl SMTP-Fehler pro Sitzung	Legt fest, wie viele Protokollfehler, z. B. Syntaxfehler, der sendende SMTP-Server verursachen darf, bevor der SMTP-Service die Beendigung der Verbindung erzwingt.
Mailer-Domäne überprüfen	Wählen Sie aus, ob der SMTP-Service die Domäne der E-Mail-Adresse des Absenders, wie mit dem Befehl MAIL FROM angegeben, mithilfe einer DNS-Suche nach einem MX-Eintrag überprüfen soll. Der SMTP-Service nimmt in diesem Fall ausschließlich E-Mail-Nachrichten von Absendern an, bei denen die Domänenkomponente der E-Mail-Adresse über einen gültigen MX-Eintrag verfügt.
Max. MTA-Hops	Definiert die maximale Anzahl von SMTP-Servern, von denen eine E-Mail-Nachricht weitergeleitet werden darf. Diese wird durch die Anzahl der Empfangsfelder im Nachrichtenheader festgelegt. Wenn diese Anzahl die angegebene Begrenzung überschreitet, weist der SMTP-Service die Übertragung zurück. Standard: 20
Umgekehrte DNS-Suche aktivieren	Wählen Sie aus, ob der SMTP-Service ermitteln soll, ob die IP-Adresse eines SMTP-Servers in einen gültigen Hostnamen aufgelöst werden kann (d. h. es ist ein DNS-Eintrag vorhanden, der auf die IP-Adresse des Peers verweist). Wenn der SMTP-Service den Hostnamen des sendenden SMTP-Servers nicht auflösen kann, werden keine E-Mail-Nachrichten von diesem SMTP-Server angenommen.

Option	Bezeichnung
Return Path-Domänenprüfung	Wählen Sie aus, ob der SMTP-Service überprüfen soll, ob die Domänenkomponente der E-Mail-Adresse des Absenders, wie im Befehl MAIL FROM angegeben, mit RFC2821, Abschnitt 4.1.2, konform ist. Dies bedeutet, dass die Domänenkomponente nur Buchstaben, Zahlen, Bindestriche und Punkte in einem bestimmten Format enthält.
HELO-Domänenprüfung	Wählen Sie aus, ob der SMTP-Service überprüfen soll, ob das mit dem Befehl "HELO/EHLO" angegebene Argument mit RFC2821, Abschnitt 4.1.2, konform ist. Dies bedeutet, dass die Domänenkomponente nur Buchstaben, Zahlen, Bindestriche und Punkte in einem bestimmten Format oder eine in eckigen Klammern eingeschlossene IP-Adresse enthält.
Forward Path-Domänenprüfung	Wählen Sie aus, ob der SMTP-Service überprüfen soll, ob die Domänenkomponente der E-Mail-Adresse des Empfängers, wie im Befehl RCPT TO angegeben, mit RFC2821, Abschnitt 4.1.2, konform ist. Dies bedeutet, dass die Domänenkomponente nur Buchstaben, Zahlen, Bindestriche und Punkte in einem bestimmten Format enthält.
SMTP-Begrüßung	Legt die Willkommensnachricht (Begrüßung) fest, die der SMTP-Service an einen SMTP-Client sendet, wenn eine Verbindung aufgebaut wird. Mit dieser Nachricht wird signalisiert, dass der SMTP-Service bereit ist, Befehle zu verarbeiten.
Empfänger Header	Der SMTP-Service fügt im Header (Empfangsfeld) der E-Mail-Nachricht bestimmte Informationen hinzu, z. B. darüber, wann und durch wen die E-Mail-Nachricht übertragen wurde. Sie können die Anzahl der Informationen in diesem Headerfeld steuern, indem Sie eine der folgenden Ebenen verwenden: • Standard (Client-IP wird angezeigt, Server-IP nicht): Der SMTP-Service gibt die IP-Adresse des sendenden SMTP-Servers im Headerfeld an, die eigene IP-Adresse jedoch nicht. • Ausführlich (Client-IP wird angezeigt, Server-IP wird angezeigt): Der SMTP-Service gibt sowohl die IP-Adresse des sendenden SMTP-Servers als auch die eigene IP-Adresse im Headerfeld an. • Eingeschränkt (IP-Adresse wird nicht angezeigt): Der SMTP-Service fügt im Headerfeld keine IP-Adressen hinzu (weder die eigene noch die IP-Adresse des Absenders). Wichtig: Wenn Sie den Headertyp für Empfang mit "Eingeschränkt" (keine IP wird angezeigt) angeben und dann Ports in Ihrer unternehmensweiten Firewall für den Empfang von SMTP-Datenverkehr öffnen, funktionieren die Analysemodule des Sender Policy Framework nicht, da diese Module auf Informationen im empfangenen Header angewiesen sind.

Einstellungen für Transport Layer Security (TLS) konfigurieren

Dieser Abschnitt beschreibt die Vorgehensweise bei der Konfiguration von Optionen, die das Verhalten des SMTP-Service beeinflussen, wenn TLS von einem anderen SMTP-Client angefordert wird.

Vorbereitende Schritte

Um die in der folgenden Prozedur beschriebenen Optionen zu verwenden, müssen Sie ein SMTP-TLS-Zertifikat installieren. Weitere Informationen finden Sie im Abschnitt *TLS-Zertifikate hochladen*.

Vorgehensweise

1. Klicken Sie im Navigationsfenster auf **SMTP > Konfiguration**.
2. Klicken Sie auf die Registerkarte **Verschlüsselung (TLS)**.
3. Aktivieren Sie die folgenden Einstellungen, wenn Sie TLS verwenden möchten:

Option	Bezeichnung
Zertifikate anfordern	Weist den SMTP-Service an, ein Zertifikat vom SMTP-Server anzufordern. Wenn der SMTP-Server kein Zertifikat ausweist, wird die Zustellung von E-Mail-Nachrichten von diesem Server untersagt.
Zertifikate überprüfen	Wenn diese Option aktiviert ist, versucht der SMTP-Service das Zertifikat des SMTP-Servers zu überprüfen (falls ein Zertifikat gesendet wurde). Wenn der Überprüfungsvorgang fehlschlägt, nimmt der SMTP-Service keine E-Mail-Nachrichten vom SMTP-Server an.
Selbst signierte Zertifikate zulassen	Der SMTP-Service akzeptiert ein Zertifikat von SMTP-Servern, die nicht von einer Zertifizierungsstelle signiert wurden (z. B. VeriSign, GlobalSign, CAcert).
TLS immer versuchen	Wenn die Funktion aktiviert ist, verwendet der SMTP-Service bei der SMTP-Kommunikation Transport Layer Security (TLS). Auch bekannt als opportunistisches TLS. Der Server versucht mithilfe des TLS-Protokolls, eine Verbindung zum Zielservers herzustellen. Wenn der Zielservers TLS unterstützt, ist der SMTP-Datenverkehr verschlüsselt. Wenn TLS nicht vom Zielservers unterstützt wird, stellt das System wieder auf unverschlüsselte Übertragung um, es sei denn, für das Zustellen einer bestimmten E-Mail-Nachricht ist ausdrücklich TLS erforderlich (angefordert von einem Response-Objekt des Richtliniensystems). In diesem Fall stellt der SMTP-Service die E-Mail-Nachricht nicht zu und sendet eine Benachrichtigung an den Absender.

Achtung: Die Unterstützung der TLS-Verschlüsselung für den Empfang von E-Mail-Nachrichten wird im SMTP-Service nur aktiviert, wenn Sie auf der Seite für TLS-Zertifikate (**SMTP > TLS-Zertifikate**) eine Schlüsseldatei und ein Zertifikat hochladen.

IP-Adressen für lokale Domänen und Relay-Hosts definieren

Dieser Abschnitt beschreibt die Vorgehensweise bei der Bestimmung des Domänen- und IP-Nummernbereichs für Ihr Unternehmen sowie bei der Einrichtung von Relay-Hosts, die alle ausgehenden E-Mail-Nachrichten über einen bestimmten E-Mail-Host leiten.

Vorgehensweise

1. Klicken Sie im Navigationsfenster auf **SMTP > Konfiguration**.
2. Klicken Sie auf die Registerkarte **Empfangender SMTP > Einstellungen**.
3. Stellen Sie folgende Informationen für lokale Domänen bereit:

Option	Bezeichnung
Domäne	Definiert die Domänenkomponente einer E-Mail-Adresse (z. B. example.com in joe@example.com), für die der SMTP-Service E-Mail-Nachrichten annimmt Anmerkung: Wenn der Eintrag example.com verwendet wird, werden E-Mail-Nachrichten von Unterdomänen von example.com (z. B. department.example.com) möglicherweise nicht durch den SMTP-Service angenommen. Wenn Sie festlegen möchten, dass der SMTP-Service E-Mail-Nachrichten für bestimmte Unterdomänen annehmen soll, müssen Sie einen separaten Eintrag für die entsprechende Unterdomäne hinzufügen. Wenn der SMTP-Service E-Mail-Nachrichten für alle Unterdomänen annehmen soll, müssen Sie zusätzlich den Eintrag .example.com hinzufügen.
Mailserver	Gibt die IP-Adresse oder den Hostnamen eines SMTP-Servers an, an den E-Mail-Nachrichten von einer bestimmten Domäne nach der Analyse weitergeleitet werden sollen Verwenden Sie einen einzelnen Eintrag oder eine durch Semikolon (;) getrennte Liste von Einträgen. Wenn eine Liste vorhanden ist, führt der SMTP-Service eine Funktionsübernahme aus, wenn der erste Host in der Liste nicht verfügbar ist. Wenn die Liste das Präfix # enthält, verteilt der SMTP-Service die E-Mail-Nachrichten an alle in der Liste angegebenen SMTP-Server.

4. Stellen Sie folgende Informationen für Relay-Hosts bereit:

Option	Bezeichnung
IP-Adresse	Gibt die IP-Adresse eines Hosts oder Netzes an, der/das E-Mail-Nachrichten an Lotus Protector for Mail Security weiterleiten darf
Subnetzmaske	Definiert einen Bereich von IP-Adressen innerhalb eines Netzes, die E-Mail-Nachrichten weiterleiten dürfen

Anmerkung: Der Eintrag 127.0.0.1/255.255.255.255 darf nicht gelöscht werden, da dieser von Lotus Protector for Mail Security verwendet wird, um E-Mail-Nachrichten, wie Quarantäneberichte oder Unzustellbarkeitsberichte (NDR), zu generieren und anderen Hosts zuzustellen.

Beispiel: Wenn ein einzelner Host E-Mail-Nachrichten an Lotus Protector for Mail Security weiterleiten soll, fügen Sie die IP-Adresse dieses Hosts (z. B. 192.168.123.100) hinzu und verwenden Sie die Subnetzmaske "255.255.255.255" für diesen Eintrag.

Wenn ein vollständiges Netz der Klasse C an Lotus Protector for Mail Security weitergeleitet werden soll, verwenden Sie die IP-Adresse 192.168.123.0 mit der Subnetzmaske 255.255.255.0.

Globale IP-Zugriffsliste konfigurieren

In diesem Thema wird erläutert, wie Sie eine Liste von IP-Adressen konfigurieren, denen beim Start einer eingehenden SMTP-Verbindung der Zugriff erlaubt oder verweigert wird.

Informationen zu diesem Vorgang

Das Verhalten der globalen IP-Zugriffsliste wird auch davon beeinträchtigt, ob Sie Grenz-IP-Adressen verwenden, bei denen es sich um IP-Adressen handelt, die die Außengrenzen des vertrauenswürdigen Netzes um Lotus Protector for Mail Security angeben. Lesen Sie das Thema „DNSBL-Einstellungen konfigurieren“ auf Seite 29, um weitere Informationen zur Verwendung von Grenz-IP-Adressen zu erhalten.

Vorgehensweise

1. Klicken Sie im Navigationsfenster auf **SMTP > Konfiguration**.
2. Klicken Sie auf die Registerkarte **Empfangender SMTP > Globale IP-Zugriffsliste**.
3. Geben Sie im Abschnitt **Zulassungsliste** eine Liste von Hosts oder Netzen an, denen Zugriff auf den SMTP-Server gewährt wurde:

Option	Bezeichnung
IP-Adresse	Gibt die IP-Adressen an, denen Zugriff auf den SMTP-Server gewährt wurde. Verwenden Sie die CIDR-Benachrichtigung, um einen Block von IP-Adressen anzugeben. Beispiel: 123.123.123.123/14. Der Eintrag nach dem Schrägstrich ist die Länge des Präfix und entspricht einer Zahl zwischen 1 und 32.
Subnetzmaske	Gibt einen Bereich betroffener Systeme für die Subnetzmaske der IP-Adresse an, die zuvor eingegeben wurde.

Wenn Sie der Zulassungsliste eine IP-Adresse hinzufügen, wird jede IP-Adresse von diesem Absender von weiteren IP-basierten Überprüfungen ausgeschlossen (beispielsweise DNSBL-Überprüfungen auf SMTP-Ebene, Überprüfungen der dynamischen Hostreputation auf SMTP-Ebene und RBL/DNSBL-Überprüfungen auf Richtlinienenebene). Die IP-Adressen in der Zulassungsliste haben Vorrang vor den IP-Adressen in der Zurückweisungsliste.

Beispiel:

Zurückweisungsliste verwendet 123.123.123.0/24 (123.123.123.1 - 123.123.123.255)

Zulassungsliste verwendet 123.123.123.123/32

Lotus Protector for Mail Security weist den Zugriff für 123.123.123.1 - 123.123.123.122 zurück, erlaubt den Zugriff für 123.123.123.123 und weist den Zugriff für 123.123.123.124 - 123.123.123.254 zurück.

4. Fügen Sie im Abschnitt **Zurückweisungsliste** Hosts oder Netzwerke manuell einer Liste von Systemen zu, denen der Zugriff auf den SMTP-Server nicht erlaubt wurde:

Option	Bezeichnung
IP-Adresse	Gibt die IP-Adressen an, denen der Zugriff auf den SMTP-Server nicht gewährt wurde und die keine Erlaubnis haben, eine Verbindung herzustellen. Verwenden Sie die CIDR-Benachrichtigung, um einen Block von IP-Adressen anzugeben. Beispiel: 123.123.123.123/14. Der Eintrag nach dem Schrägstrich ist die Länge des Präfix und entspricht einer Zahl zwischen 1 und 32.
Subnetzmaske	Gibt den Bereich betroffener Systeme für die Subnetzmaske der eingegebenen IP-Adressen an.

Handhabung der Zurückweisung von IP-Adressen auf der Zurückweisungsliste:

- Mit Fehler zurückweisen: Der SMTP-Service weist die Zustellung von E-Mail-Nachrichten vom Absender zurück und gibt den angegebenen Fehlercode mit der definierten Fehlermeldung an.
- Ohne Hinweis löschen: Der SMTP-Service gibt eine eingehende E-Mail-Nachricht zurück, benachrichtigt den Absender der E-Mail jedoch nicht darüber, dass die E-Mail abgelehnt wurde. Mit dieser Methode wird verhindert, dass gültige E-Mail-Adressen von Spammern durchsucht werden.

DNSBL-Einstellungen konfigurieren

Dieser Abschnitt beschreibt die Vorgehensweise bei der Konfiguration einer Liste mit IP-Adressen, die blockiert werden, weil sie den Versand von Spam zulassen. Ebenso wird beschrieben, wie Quoten für die verfügbaren DNSBL-Server (Domain Name Server Block List) in Ihrem Netz festgelegt werden.

Informationen zu diesem Vorgang

DNSBL-Grenz-IPs sind IP-Adressen, die die äußerste Grenze des vertrauenswürdigen Netzes Lotus Protector for Mail Security angeben. In der folgenden Tabelle sind die IP-Adressen aufgeführt, die als DNSBL-Grenz-IP-Adressen für Lotus Protector for Mail Security gelten:

Tabelle 16. DNSBL-Grenz-IP-Adressen

DNSBL-Grenz-IP-Adresse	Position
Server, die an lokale Domänen weiterleiten	SMTP > Konfiguration > Empfangender SMTP > Einstellungen > Lokale Domänen
Server, die über Lotus Protector for Mail Security weiterleiten	SMTP > Konfiguration > Empfangender SMTP > Einstellungen > Relay-Hosts
Server, an die Lotus Protector for Mail Security weiterleitet	SMTP > Konfiguration > Sender SMTP > Zustellung > Weiterleiten
Eine benutzerdefinierte, durch Semikolon getrennte Liste von IP-Adressen	host_reputation.border_ips

Wichtig: Sie können IP-Grenzadressen verwenden, wenn Lotus Protector for Mail Security E-Mail-Nachrichten direkt von Hosts im Internet empfängt. Sie können jedoch keine Grenz-IP-Adressen verwenden, wenn Lotus Protector for Mail Security sich hinter einem SMTP-Relay befindet.

Vorgehensweise

1. Klicken Sie im Navigationsfenster auf **SMTP > Konfiguration**.
2. Klicken Sie auf die Registerkarte **Empfangender SMTP > DNSBL-Einstellungen**.
3. Aktivieren Sie das Kontrollkästchen **Aktivieren**.
4. Geben Sie einen Fehlercode und eine Fehlernachricht ein.

5. Klicken Sie auf die Schaltfläche **DNSBL-Einstellungen**.
6. Geben Sie im Bereich **DNSBL-Listen** einen Schwellenwert ein. Wenn die Summe aller DNSBL-Ser-
verübereinstimmungsquoten diesen Wert übersteigt, wird die analysierte E-Mail-Nachricht für das
Spam-DNSBL-Analysemodul als Übereinstimmung gewertet.
7. Klicken Sie auf **Hinzufügen**.
8. Aktivieren Sie das Kontrollkästchen **Aktiviert**.
9. Geben Sie den Namen des DNSBL-Servers und die Übereinstimmungsquote ein. Die Übereinstim-
mungsquote gibt den Wert an, der zur Gesamtquote hinzugerechnet wird, wenn dieser DNSBL-Ser-
ver ein positives Ergebnis zurückgibt. Dieser Wert kann zur Feinabstimmung des Mechanismus ver-
wendet werden, wenn Sie DNSBL-Server mit unterschiedlichen Zuverlässigkeiten verwenden.
10. Klicken Sie auf **OK** und anschließend auf **Änderungen speichern**.

Empfängerüberprüfung konfigurieren

Mithilfe der Empfängerüberprüfung blockiert der SMTP-Service umgehend E-Mail-Nachrichten, die an ei-
nen Benutzer gesendet wurden, der in Ihrem Unternehmen nicht existiert.

Vorgehensweise

1. Klicken Sie im Navigationsfenster auf **SMTP > Konfiguration**.
2. Klicken Sie auf die Registerkarte **Empfangender SMTP > Empfängerüberprüfung**.
3. Aktivieren Sie das Kästchen **Empfängerüberprüfung aktivieren**.
4. Wählen Sie aus, wie Lotus Protector for Mail Security zurückgewiesene Empfänger verarbeiten soll:

Option	Bezeichnung
Mit Fehler zurückweisen	Lotus Protector for Mail Security gibt den angegebenen Fehlercode und die angegebene Fehlernachricht an den SMTP-Client zurück. Der Absender erfährt, welche SMTP-Adressen gültig sind bzw. welches Verhalten akzeptabel oder inakzeptabel sein kann.
Ohne Hinweis löschen	Der SMTP-Service weist eine eingehende E-Mail-Nachricht zurück, benachrichtigt den Absender der E-Mail jedoch nicht darüber, dass die E-Mail abgelehnt wurde. Mit dieser Methode wird verhindert, dass gültige E-Mail-Adressen von Spammern durchsucht werden.

5. Geben Sie einen SMTP-Fehlercode und eine SMTP-Fehlernachricht ein.
6. Wählen Sie einen Zugriffstyp für die Empfänger:

Option	Bezeichnung
Verweigert	Alle Empfänger, die nicht auf der Empfängerliste stehen, werden abgewiesen.
Zugelassen	Alle Empfänger, die nicht auf der Empfängerliste stehen, werden zugelassen. Sie können entweder eine Liste von zugelassenen Empfängern erstellen und alle anderen abweisen oder eine Liste von abgewiesenen Empfängern erstellen und alle anderen zulassen.

Achtung: Sie können für die Empfängerüberprüfung auch benutzergenerierte SMTP-Domänenlisten und SMTP-Adresslisten verwenden. Sie müssen die Liste der Dateinamen (durch Kommas getrennte Liste einschließlich des vollständigen Pfads) zur Datei `/etc/recipientverificationd.conf` hinzufügen.

Alle Dateien im Verzeichnis `/var/lib/recipientverificationd` werden gelöscht, wenn Sie eine Konfiguration speichern. Sie sollten ein anderes Verzeichnis verwenden, z. B. `/var/lib/recipientverificationd/user`.

Analyse der Nullebene (ZLA, Zero Level Analysis) aktivieren

Die Analyse der Nullebene (ZLA) ist eine Klassifizierungsmethode, die Lotus Protector for Mail Security für eingehende E-Mail-Nachrichten verwendet.

Informationen zu diesem Vorgang

Während viele unerwünschte E-Mail-Nachrichten in einem frühen Stadium der Nachrichtenübermittlung zurückgewiesen werden, werden bei der ZLA-Analyse die Nachrichten bereits während der Übertragung analysiert. Dabei werden sie vom SMTP-Service entweder zurückgewiesen oder gelöscht.

Vorgehensweise

1. Klicken Sie im Navigationsfenster auf **SMTP > Konfiguration**.
2. Wählen Sie die von ZLA zu verwendende Kategorie zur Erkennung eingehender E-Mail-Nachrichten aus:

Kategorie	Beschreibung
Spam	Kennzeichnet Typen von Massen-E-Mail-Nachrichten, wie Phishing, Werbung oder Malware
Unzustellbarkeitsberichte	Unzustellbarkeitsberichte werden an den Absender als Antwort auf die fehlgeschlagene Übertragung einer E-Mail-Nachricht gesendet, um diesem mitzuteilen, dass der angegebene Empfänger die Nachricht nicht erhalten hat. Spammer verwenden häufig gefälschte E-Mail-Adressen als Absender von E-Mail-Nachrichten. Wenn ein Server diesen Nachrichtentyp zurückweist (beispielsweise, weil der Empfänger der Nachricht nicht vorhanden ist), kann das dazu führen, dass der Besitzer einer gefälschten Adresse irrtümlicherweise viele Nichtzustellungsberichte erhält. Achtung: Seien Sie vorsichtig, wenn Sie eine Response für diese Kategorie auswählen. Viele Unzustellbarkeitsberichte sind möglicherweise berechtigt, beispielsweise, wenn ein Absender einer E-Mail-Nachricht die E-Mail-Adresse des Empfängers falsch geschrieben hat.

3. Definiert, wie der SMTP-Service E-Mail-Nachrichten aus einer bestimmten Kategorie verarbeiten soll:

Response	Beschreibung
Nachricht blockieren	Ist diese Option ausgewählt, antwortet der SMTP-Service mit einer Fehlnachricht auf der SMTP-Ebene an den Versuch des Absenders. Diese Nachricht gibt an, dass die Übertragung dieser E-Mail-Nachricht zurückgewiesen wurde.

Response	Beschreibung
Ohne Hinweis löschen	Wenn diese Option aktiviert wird, weist der SMTP-Service eine eingehende E-Mail-Nachricht zurück, benachrichtigt den Absender der E-Mail jedoch nicht darüber, dass die E-Mail abgelehnt wurde. Mit dieser Methode wird verhindert, dass gültige E-Mail-Adressen von Spammern durchsucht werden.
Als Spam markieren	Ist diese Option ausgewählt, fügt der SMTP-Service der E-Mail-Nachricht ein neues Headerfeld X-ZLA-Header hinzu. Gültige Werte für dieses Feld sind: • Spam: Gibt an, dass eine E-Mail-Nachricht als unerwartete Massen-E-Mail (Spam) klassifiziert wurde. • NDR: Gibt an, dass eine E-Mail-Nachricht als Unzustellbarkeitsbericht (NDR) klassifiziert wurde. Jeder Wert verfügt über das Suffix ; xxxx, das Informationen zu dem verwendeten Analysemodul bereitstellt. Tipp: Das Hinzufügen eines Headerfelds zu einer E-Mail-Nachricht kann in Kombination mit dem Richtlinienensystem möglicherweise nützlich sein. Sie können eine neue Regel hinzufügen, die das Analysemodul der Nachrichtenfeldüberprüfung enthält. Dieses Analysemodul ermittelt E-Mail-Nachrichten eines bestimmten Typs und gibt an, wie diese Nachrichten verarbeitet werden sollen (ob sie zum Beispiel in einem Quarantänespeicher gespeichert werden sollen). Anmerkung: Diese Response kann möglicherweise geringe Auswirkungen auf die Leistung von Lotus Protector for Mail Security haben, da durch sie eingehende E-Mail-Nachrichten geändert werden.
Keins	Ist diese Option ausgewählt, werden E-Mail-Nachrichten von dem SMTP-Service angenommen, jedoch von ZLA nicht geändert.

4. Konfigurieren Sie in den Blockiereinstellungen, wie der SMTP-Service E-Mail-Nachrichten zurückweisen soll, bei denen ZLA ermittelt hat, dass sie zu einer der angegebenen Kategorien gehören, denen die Response "BLOCK" zugewiesen wurde. SMTP-Server protokollieren entweder eine Fehlermeldung oder senden einen Unzustellbarkeitsbericht an den Absender einer E-Mail-Nachricht. Sie sollten eine aussagekräftige Beschreibung für den Grund angeben, aus dem eine E-Mail-Nachricht von Lotus Protector for Mail Security zurückgewiesen wurde. Die an den Absender gesendeten Fehlerantworten enthalten einen numerischen Fehlercode, gefolgt von einer Beschreibung oder einem Kommentar. Beispiel: 550 Blockiert durch ZLA.

Option	Bezeichnung
Fehlercode	Definiert den numerischen Fehlercode, der von ZLA verwendet werden soll, wenn eine E-Mail-Nachricht ermittelt wird, die zurückgewiesen werden soll Achtung: Die in SMTP-Antworten verwendeten numerischen Fehlercodes sind in RFC 2821 im Abschnitt 4.2 mit dem Titel "SMTP Replies" (SMTP-Antworten) vordefiniert. Da SMTP-Server diesen Code zur Verwaltung ihres aktuellen Status verwenden, sollten Sie sicherstellen, dass Sie einen mit diesen Definitionen kompatiblen Wert auswählen. Ein Antwortcode, der mit dem Wert 4yz beginnt, kennzeichnet beispielsweise einen temporären Fehler, während ein Antwortcode, der mit dem Wert 5yz beginnt, einen permanenten Fehler kennzeichnet.
Fehlernachricht	Definiert die Beschreibung bzw. den Kommentar zu dem Fehler. Anmerkung: Da SMTP ASCII-Zeichen verwendet, sollten Sie sicherstellen, dass in Ihrer Beschreibung bzw. in Ihrem Kommentar nur Zeichen aus dem ASCII-Zeichensatz enthalten sind.

Dynamischen Hostreputationsfilter konfigurieren

Dieser Abschnitt beschreibt die Vorgehensweise bei der Konfiguration von Lotus Protector for Mail Security, um einen Einstufungsmechanismus für die Hostreputation zu verwenden, der bestimmt, ob eine eingehende E-Mail-Nachricht zurückgewiesen werden sollte, ausgehend davon, ob der E-Mail-Absender bereits zuvor Spamnachrichten versendet hat.

Informationen zu diesem Vorgang

Da dieser Mechanismus auf den IP-Adressen verbundener Hosts basiert, müssen Sie eine Liste von IP-Grenzadressen konfigurieren, wenn Sie zusätzliche SMTP-Relays verwenden, die E-Mail-Nachrichten aus dem Internet empfangen und an Lotus Protector for Mail Security weiterleiten. Andernfalls werden die internen SMTP-Relays möglicherweise der Liste abgelehnter Hosts hinzugefügt und E-Mail-Nachrichten werden nicht an Lotus Protector for Mail Security weitergeleitet.

Vorgehensweise

1. Klicken Sie im Navigationsfenster auf **SMTP > Konfiguration**.
2. Klicken Sie auf die Registerkarte **Empfangender SMTP > Dynamischer Hostreputationsfilter**.
3. Aktivieren Sie das Kontrollkästchen **Dynamische Hostreputation aktivieren**.
4. Wählen Sie im Bereich **Handhabung abgewiesener Hosts** die Methode aus, mit der der SMTP-Service die E-Mail-Nachricht abweisen soll:

Option	Bezeichnung
Mit Fehler zurückweisen	Der SMTP-Service weist Zustellungen von E-Mail-Nachrichten eines aufgeführten SMTP-Clients zurück und gibt den angegebenen Fehlercode mit der definierten Fehlermeldung an den SMTP-Client zurück. Anmerkung: SMTP-Clients versuchen möglicherweise wiederholt, eine E-Mail-Nachricht zuzustellen, wenn frühere Zustellversuche erfolglos waren. Diese Clients können verfügbare gleichzeitig bestehende Verbindungen zum SMTP-Service monopolisieren.
Ohne Hinweis löschen	Der SMTP-Service gibt eine eingehende E-Mail-Nachricht zurück, benachrichtigt den Absender der E-Mail jedoch nicht darüber, dass die E-Mail abgelehnt wurde. Mit dieser Methode wird verhindert, dass gültige E-Mail-Adressen von Spammern durchsucht werden. Beispiel: Ein Absender wird vom dynamischen Hostreputationsfilter als Spammer erkannt. Wenn Sie die Option Mit Fehler zurückweisen auswählen, erhält der Absender die Fehlermeldung: "550 Sie werden als Spammer aufgelistet (123.123.213.123)" oder eine andere Nachricht, die Sie als Antwort konfiguriert haben. Wenn Sie die Option Ohne Hinweis löschen auswählen, erhält der Sender die Meldung: "220 Willkommen bei...." und kommuniziert mit Lotus Protector for Mail Security, obgleich der Absender als Spammer bekannt ist. Anmerkung: Mit der Option "Mit Fehler zurückweisen" lassen sich Verbindungshosts besser handhaben, da sie die Verbindung bei hohem Datenverkehr oder hoher Auslastung früher unterbricht.
Markierung	Wenn sich die IP-Adresse des SMTP-Clients in der Liste abgelehnter Hosts befindet, wird das folgende Headerfeld vom Filter in die E-Mail-Nachricht eingefügt: X-MSHostReputation:<IP-Adresse des Absenders>

5. Konfigurieren Sie im Bereich **Dynamische Hostreputationskonfiguration** den Filter so, dass er die IP-Adressen von Hosts, die einen hohen Spamanteil senden, unter Quarantäne stellt:

Option	Bezeichnung
Analysefenster (Minuten)	Legt fest, wie lange die Klassifizierungen analysierter E-Mail-Nachrichten von Lotus Protector for Mail Security beibehalten werden sollen, um anhand der nachfolgenden Kriterien festzulegen, ob ein SMTP-Client unter Quarantäne gestellt werden soll
Quarantänedauer (Minuten)	Legt fest, wie lange ein Host unter Quarantäne gestellt wird. Während dieser Zeit dürfen keine E-Mail-Nachrichten vom Host zugestellt werden.
Mindesttreffer für Spam/Phishing	Gibt die Mindestanzahl von Spam- oder Phishing-E-Mail-Nachrichten an, die von Lotus Protector for Mail Security für eine ordnungsgemäße Einstufung benötigt werden
Spam-/Phishing-Prozentsatz	Legt das Verhältnis von Spam- oder Phishing-E-Mail-Nachrichten zu anderen E-Mail-Nachrichten fest, das darüber entscheidet, ob ein Host als Spammer eingestuft wird

6. Klicken Sie auf **Änderungen speichern**.

Ausgehende E-Mail-Nachrichten aus Ihrem Netz einrichten

Dieser Abschnitt beschreibt die Vorgehensweise beim Einrichten des SMTP-Service zum Versenden von E-Mail-Nachrichten an interne und externe SMTP-Server. Zudem wird die Vorgehensweise beim Einrichten des SMTP-Service zur Verarbeitung von Zustellungsproblemen beschrieben.

Vorgehensweise

1. Klicken Sie im Navigationsfenster auf **SMTP > Konfiguration**.
2. Klicken Sie auf die Registerkarte **Sender SMTP > Einstellungen**.
3. Aktivieren Sie das Kontrollkästchen **Aktivieren**.
4. Stellen Sie folgende Informationen bereit:

Option	Bezeichnung
Protokollierung aktivieren	Weist den SMTP-Service an, einen Protokolleintrag für jede erfolgreiche Zustellung einer E-Mail-Nachricht in eine Protokolldatei zu schreiben Diese Protokolldatei hat den Namen smtp-jjjjmmmtt0000. Anmerkung: Sie können auf die SMTP-Protokolldateien mithilfe des Browsers für Protokolldateien unter System > Protokolldateien zugreifen.
HELO-Domäne	Definiert, wie der SMTP-Service sich gegenüber anderen SMTP-Servern durch Anwendung des HELO-/EHLO-SMTP-Befehls ausweist. Dabei wird typischerweise der Hostname von Lotus Protector for Mail Security verwendet.
Spoolfehler entfernen	Wenn diese Option aktiviert ist, werden E-Mail-Nachrichten gelöscht, die nach der maximalen Anzahl von Zustellversuchen (entsprechend der Option Maximale Anzahl der Wiederholungen) nicht zugestellt werden konnten. Wenn diese Option deaktiviert ist, werden diese E-Mail-Nachrichten in die Warteschlange <i>frozen</i> verschoben und verbleiben dort für die Anzahl von Tagen, die auf der Registerkarte "Wartung" angegeben wurde.
Zustellungsverzögerung	Gibt die Zeitspanne an, die der SMTP-Service zwischen seinem ersten und zweiten Zustellversuch warten soll. Jeder nachfolgende Zustellungsversuch erfolgt mit einer verdoppelten Zustellungswartezeit im Vergleich zum vorherigen Versuch (z. B. 240 Sekunden -> 480 Sekunden -> 960 Sekunden -> usw.). Sie können die Wartezeit zwischen den Versuchen ändern, indem Sie die Option Inkrementfaktor für erneutes Senden ändern.
Maximale Anzahl der Wiederholungen	Legt die maximale Anzahl der Wiederholungen pro E-Mail-Nachricht fest, bevor dem Sender der E-Mail-Nachricht ein Unzustellbarkeitsbericht gesendet wird und die E-Mail-Nachricht in die Warteschlange <i>frozen</i> verschoben wird

Option	Bezeichnung
Inkrementfaktor für erneutes Senden	Diese Einstellung wirkt sich auf die Wartezeit zwischen zwei Zustellversuchen aus. Sie können die folgenden Werte festlegen: • 0 = Jeder Zustellversuch wird mit einem festen Zeitintervall verzögert, das im Feld Zustellungsverzögerung angegeben ist. • 1 = Jeder Zustellversuch wird mit einer verdoppelten Wartezeit im Vergleich zum vorherigen Zustellversuch durchgeführt (Standardeinstellung). • >1 (größer als 1) = Jeder Zustellversuch wird mit einer Gesamtwartezeit durchgeführt, die sich aus der Summe der Wartezeit des vorherigen Zustellversuchs und dem vorherigen Zustellversuch geteilt durch n ergibt (wobei n der gewählte Wert ist). Die Formel für die Wartezeit der Zustellversuche lautet $T(i) = T(i-1) + T(i-1) / n$, wobei $T(i)$ die Wartezeit des Zustellversuchs des iten Versuchs ist und die Basisanweisung $T(1)$ mit dem Wert der Option Zustellungsverzögerung festgelegt ist. Achtung: Wenn Sie diesen Wert ändern, kann dies drastische Auswirkungen auf die Zeitspanne haben, die sich eine E-Mail-Nachricht in der Warteschlange <i>resend</i> befindet. Werden beispielsweise die Standardwerte der Option Zustellungsverzögerung (240 Sekunden) und der Option Maximale Anzahl der Wiederholungen (8 Wiederholungen) verwendet und wird dann der Wert für den Inkrementfaktor für erneutes Senden auf 2 geändert, wartet die E-Mail-Nachricht 197 Minuten in der Warteschlange <i>resend</i>, statt 1020 Minuten, die sie bei einem Wert von 1 gewartet hätte. Die Werte der Option Zustellungsverzögerung und der Option Maximale Anzahl der Wiederholungen müssen entsprechend angepasst werden.
Absender bei Wiederholungen benachrichtigen	Definiert die Anzahl der fehlgeschlagenen Zustellversuche, bevor der Absender der E-Mail-Nachricht über temporäre Zustellungsprobleme benachrichtigt wird
Anzahl der aufgeführten Zeilen bei automatischem Wiederanlauf	Legt die Anzahl der Zeilen einer unzustellbaren E-Mail-Nachricht fest, die der Unzustellbarkeitsbericht an den Absender enthalten soll

Option	Bezeichnung
Zustellung	Wählen Sie aus, wie der SMTP-Service den nächsten SMTP-Server festlegen soll, an den eine E-Mail-Nachricht weitergeleitet wird: • DNS-Auflösung: Legt den SMTP-Zielserver durch Auffinden von DNS MX-Einträgen fest. Dieser Service verwendet die DNS-Standardserver, so wie sie auf der Seite Netzwerk konfiguriert sind, es sei denn, bestimmte DNS-Server wurden dieser Liste hinzugefügt. • Weiterleiten: Leitet ausgehende E-Mail-Nachrichten an einen SMTP-Server gemäß den Konfigurationen in der Liste weiter Sie können E-Mail-Nachrichten entweder an eine bestimmte Domäne weiterleiten, indem Sie den Domänennamen der IP-Adresse oder dem Hostnamen eines SMTP-Relays zuordnen (z. B. example.com zu Relay0.mycompany.com), oder an ein Platzhalterzeichen * in Verbindung mit einer bestimmten Domäne (zum Beispiel *.example.com zu Relay1.mycompany.com), um Unterdomänen an einen bestimmten Relay weiterzuleiten, oder an ein Platzhalterzeichen *, um den gesamten Ausgangsdatenverkehr durch einen bestimmten Relay weiterzuleiten. Die Option Mail-Server kann für eine Funktionsübernahme eine durch Semikolons (;) getrennte Liste von SMTP-Servern enthalten. Wenn die Liste das Präfix # enthält, verteilt der SMTP-Service die E-Mail-Nachrichten an alle vorgegebenen SMTP-Server. Anmerkung: Wenn der SMTP-Service für eine bestimmte Domäne kein konfiguriertes Relay findet, stellt er sich für diese Domäne auf DNS-Auflösung zurück.

5. Klicken Sie auf **Änderungen speichern**.

Unzustellbare E-Mail-Nachrichten und SMTP-Protokolldateien aus dem Dateisystem entfernen

Dieser Abschnitt beschreibt die Vorgehensweise beim Einrichten der Anzahl der Tage, für die Lotus Protector for Mail Security unzustellbare E-Mail-Nachrichten oder SMTP-Protokolldateien im Dateisystem speichern soll.

Vorgehensweise

1. Klicken Sie im Navigationsfenster auf **SMTP > Konfiguration**.
2. Klicken Sie auf die Registerkarte **Verwaltung**.
3. Stellen Sie folgende Informationen bereit:

Option	Bezeichnung
Tage, die unzustellbare Nachrichten aufbewahrt werden sollen	Legt fest, wie viele Tage nicht zustellbare E-Mail-Nachrichten gespeichert werden sollen, bevor sie aus dem System gelöscht werden Anmerkung: Lotus Protector for Mail Security speichert nicht zustellbare E-Mail-Nachrichten nur, wenn das Kontrollkästchen Spoolfehler entfernen auf der Registerkarte SMTP > Konfiguration > Sender SMTP nicht aktiviert ist.
Tage, die Protokolldateien aufbewahrt werden sollen	Legt fest, wie viele Tage SMTP-Protokolldateien gespeichert werden sollen, bevor sie aus dem System gelöscht werden.

4. Klicken Sie auf **Änderungen speichern**.

Installation von TLS-Zertifikaten

Um den Datenverkehr zwischen Lotus Protector for Mail Security und einem SMTP-Server zu verschlüsseln, müssen Sie ein SMTP-TLS-Zertifikat installieren. Das Zertifikat kann selbst signiert, von einer anderen Stammzertifizierungsstelle ausgegeben oder von einer Zwischenzertifizierungsstelle signiert sein. Platzhalterzertifikate werden unterstützt.

Ein Serverzertifikat hochladen

Sie können Zertifikate für vertrauenswürdige SMTP-Server hochladen, mit denen der SMTP-Service kommuniziert (ihre internen SMTP-Server oder SMTP-Server in anderen Niederlassungen).

Sie können auch Zertifikate für Zertifizierungsstellen hochladen, die zur Bestätigung der Identität des Ausstellers eines Zertifikats verwendet werden, das von einem anderen SMTP-Server gesendet wurde (Zertifizierungsketten).

Sie laden eine private Schlüsseldatei und das entsprechende Zertifikat hoch, die vom SMTP-Service verwendet werden sollen. Das Zertifikat wird an den SMTP-Server gesendet, der die TLS-Verschlüsselung für die Zustellung anfordert. Das Zertifikat enthält den öffentlichen Schlüssel, mit dem die Daten zu verschlüsseln sind; die private Schlüsseldatei verbleibt bei Lotus Protector for Mail Security, um Daten zu entschlüsseln. Normalerweise wird das Zertifikat von einem vertrauenswürdigen Dritten signiert, um die Identität von Lotus Protector for Mail Security zu bestätigen, Sie können aber auch ein selbst signiertes Zertifikat verwenden.

Wenn Sie keine Schlüsseldatei und kein Zertifikat haben, können Sie anhand der Anweisungen unter <http://www.openssl.org/docs/HOWTO/keys.txt> und <http://www.openssl.org/docs/HOWTO/certificates.txt> Schlüssel/Zertifikat-Paare erstellen, die mit dem SMTP-Service von Lotus Protector for Mail Security verwendet werden können.

Beispiel: Selbst signiertes Zertifikat erstellen

1. Erstellen Sie einen privaten Schlüssel mithilfe dieses Befehls:
`$ openssl genrsa 2048 > server.key`
2. Nach Erstellen des privaten Schlüssels erstellen Sie unter Verwendung dieses Befehls eine eigene Kopie des selbst signierten Zertifikats:
`$ openssl req -new -x509 -key server.key -out server.cert`
`C:> openssl req -new -x509 -key server.key -out server.cert -config openssl.cnf`
3. Der allgemeine Name, den Sie für den Binärwert "OpenSSL" angeben, ist der vollständig qualifizierte Hostname, der auf die IP-Adresse antwortet, auf die der XMail-Server reagiert. Wenn Sie ein Zertifikat wünschen, das von einer Autorität signiert wurde, erstellen Sie mithilfe dieses Befehls eine Zertifikatsanforderungsdatei:
`$ openssl req -new -key server.key -out cert.csr`
`C:> openssl req -new -key server.key -out cert.csr -config openssl.cnf`

SMTP-TLS-Zertifikate hochladen

Vorbereitende Schritte

Sie müssen über Kopien der Zertifikatsdatei und der zugehörigen privaten Schlüsseldatei verfügen, um den Hochladevorgang abzuschließen. Das Zertifikat muss im Format Privacy Enhanced Electronic Mail (PEM) codiert sein. Weitere Informationen zum Bestimmen des Dateiformats finden Sie im Abschnitt *Dateiformat eines Zertifikats überprüfen*.

Informationen zu diesem Vorgang

Sie können ein Zertifikat/Schlüssel-Paar über die Befehlszeile oder mithilfe von Lotus Protector Manager, auch bezeichnet als lokale Verwaltungsschnittstelle (LMI = Local Management Interface), installieren.

Anmerkung: Sie können gleichzeitig nur ein Paar aus privatem Schlüssel und Zertifikat hochladen. Wenn Sie ein zusätzliches Paar hochladen, wird das vorhandene Paar überschrieben.

Vorgehensweise

- Zertifikat mithilfe von Lotus Protector Manager installieren
 1. Erweitern Sie im Navigationsfenster die Option **SMTP** und klicken Sie auf **TLS-Zertifikate**.
 2. Geben Sie die Positionen der Zertifikatsdatei und der Schlüsseldatei an und klicken Sie dann auf **Zertifikat hochladen**.
 3. Erweitern Sie im Navigationsfenster die Option **SMTP**, klicken Sie auf **Konfiguration** und dann auf **Verschlüsselung (TLS)**.
 4. Wählen Sie die Option **TLS immer versuchen** aus und klicken Sie auf **Änderungen speichern**, um opportunistisches TLS zu aktivieren.
- Zertifikat über die Befehlszeile installieren
 1. Melden Sie sich über SSH mit Rootberechtigung an der Konsole an.
 2. Benennen Sie die Dateien um. Der Name der privaten Schlüsseldatei muss `server.key` lauten. Der Name des Zertifikats muss `server.cert` lauten.
 3. Verwenden Sie den Befehl **sftp put**, um die private Schlüssel- und die Zertifikatsdatei in das folgende Verzeichnis hochzuladen: `/etc/xmail/`
 4. Verwenden Sie in diesem Verzeichnis einen Texteditor zum Öffnen der Datei `server.tab` und legen Sie für den Parameter **EnableSMTP-TLS** den Wert `1` fest.
 5. Aktivieren Sie die Änderung, indem Sie den XMail-Server erneut starten. Geben Sie über die Konsole den Befehl `service xmail restart` ein.

Nächste Schritte

Die SMTP-Verbindung ist nun durch TLS gesichert. Um die Verbindung zu überprüfen, gehen Sie wie im Abschnitt *TLS-Verbindung testen* beschrieben vor.

Zertifikat aus einer Zwischenzertifizierungsstelle hinzufügen

Sie können ein Zertifikat zum Sichern der Verbindung zum SMTP-Server verwenden, das von einer Zwischenzertifizierungsstelle signiert wurde. Sie müssen das Zertifikat der Zwischenzertifizierungsstelle zum vorhandenen Serverzertifikat hinzufügen.

Vorbereitende Schritte

Ein von einer Stammzertifizierungsstelle signiertes SMTP-TLS-Zertifikat muss installiert sein, bevor Sie ein Zertifikat von einer Zwischenzertifizierungsstelle hinzufügen können.

Informationen zu diesem Vorgang

Wenn Sie über keine Kopie des Zwischenzertifikats verfügen, müssen Sie die Details zum Unterzeichner abrufen und eine lokale Kopie herunterladen. Weist die Zertifikatsdatei nicht das PEM-Format auf, müssen Sie sie konvertieren. Weitere Informationen finden Sie im Abschnitt *Dateiformat eines Zertifikats überprüfen*.

Vorgehensweise

1. Melden Sie sich über SSH mit Rootberechtigung an der Konsole an und führen Sie vom Verzeichnis `/etc/xmail/` aus den folgenden Befehl aus: `openssl x509 -in server.cert -text -noout`
Der Befehl gibt Detailinformationen zum Zertifikat zurück, einschließlich des URI, über den Sie das Zertifikat herunterladen können. Beispiel:
Authority Information Access
CA Issuers - URI:https://ssl.trustedCA.com/ssl.crt
2. Verwenden Sie einen Browser, um die Adresse der Zertifizierungsstelle aufzurufen, und laden Sie das Zertifikat in ein temporäres Verzeichnis herunter.
3. Fügen Sie das Zertifikat zum vorhandenen Serverzertifikat hinzu.
 - a. Öffnen Sie in einem Texteditor das vorhandene Serverzertifikat und das Zertifikat, das Sie von der Zwischenzertifizierungsstelle heruntergeladen haben.
 - b. Kopieren Sie aus dem heruntergeladenen Zertifikat den Teil der Datei, der mit der Zeile `-----BEGIN CERTIFICATE-----` beginnt und mit der Zeile `-----END CERTIFICATE-----` endet.
 - c. Suchen Sie im vorhandenen Serverzertifikat die Zeile, die `-----END CERTIFICATE-----` lautet, und fügen Sie die Informationen, die Sie aus dem heruntergeladenen Zertifikat kopiert haben, direkt nach dieser Zeile ein.

Dateiformat eines Zertifikats überprüfen

Zertifikatsdateien müssen das Format Privacy Enhanced Electronic Mail (PEM) aufweisen. Sie können einen Befehl zum Überprüfen des Dateiformats ausführen und die Dateien bei Bedarf in das PEM-Format konvertieren.

Informationen zu diesem Vorgang

Wenn die Zertifikatsdatei das binäre Format Distinguished Encoding Rules (DER) aufweist, können Sie einen Befehl ausführen, um sie in das PEM-Format zu konvertieren.

Vorgehensweise

1. Um das Dateiformat zu überprüfen, geben Sie Folgendes über die Befehlszeile ein: `openssl x509 -in CERTIFICATE_NAME.crt -text -noout`

CERTIFICATE_NAME.crt ist der Name der Zertifikatsdatei.

Weist die Datei das DER-Format und nicht das PEM-Format auf, wird in der Anzeige ein Fehler ähnlich dem folgenden angezeigt:

```
Unable to load certificate
13233:error:0906D06C:PEM routines:PEM_read_bio:no start
line:pem_lib.c:644:Expecting: TRUSTED CERTIFICATE
```

2. Um eine Datei vom DER-Format in das PEM-Format zu konvertieren, geben Sie den folgenden Befehl in einer Zeile ein: `openssl x509 -inform der -in CERTIFICATE_NAME.crt -out CERTIFICATE_NAME.cert`
CERTIFICATE_NAME.crt ist der Name der Zertifikatsdatei im DER-Format.

TLS-Verbindung testen

Testen Sie die Verbindung, nachdem Sie ein Zertifikat installiert haben, um zu überprüfen, ob sie sicher ist.

Informationen zu diesem Vorgang

Mithilfe der folgenden Prozedur können Sie testen, ob die TLS-Konfiguration ordnungsgemäß funktioniert.

Vorgehensweise

1. Melden Sie sich über SSH mit Rootberechtigung an der Konsole an.
2. Geben Sie den folgenden Befehl in einer Zeile ein: `openssl s_client -starttls smtp -crlf -connect 127.0.0.1:25 -CAfile /etc/apache2/ssl.crt/ca-bundle.crt`

Wenn die Verbindung ordnungsgemäß konfiguriert ist, gibt der Befehl die folgende Ausgabe zurück:
Verify return code: 0 (ok)

SMTP-Warteschlangen

Die SMTP-Warteschlangen enthalten E-Mail-Nachrichten, die zur Verarbeitung durch Lotus Protector for Mail Security anstehen.

Warteschlange "unchecked"

Die Warteschlange *unchecked* enthält E-Mail-Nachrichten, die zur Analyse durch Lotus Protector for Mail Security anstehen.

Jede eingehende E-Mail-Nachricht wird zunächst in die Warteschlange *unchecked* gestellt. Der Status *unchecked/processing* gibt an, dass E-Mail-Nachrichten von Lotus Protector for Mail Security verarbeitet werden. Nachdem die E-Mail-Nachricht durch die geltende Richtlinie analysiert wurde, wird sie aus der Warteschlange *unchecked* entfernt.

Die E-Mail-Nachrichten in der Warteschlange *unchecked* werden als temporäre Daten behandelt. Eine umfangreiche Warteschlange *unchecked* zeigt an, dass Lotus Protector for Mail Security mehr E-Mail-Nachrichten empfängt, als verarbeitet werden können.

Die folgenden Nachrichten werden möglicherweise angezeigt, wenn es sich um eine fehlerhafte E-Mail oder sonstige Probleme handelt (diese Nachrichten dienen rein zur Information und erfordern keinen Benutzereingriff):

```
unchecked/processable
unchecked/processable.cal
unchecked/processable.smtp
unchecked/processable.timeout
unchecked/processable.processing
unchecked/processable.processing.db
unchecked/processable.processing.pgdb
unchecked/processable.processing.unk
```

Warteschlange "local"

Die Warteschlange *local* enthält E-Mail-Nachrichten, die sich zuvor in der Warteschlange *unchecked* befanden und nach ihrer Analyse aus der Warteschlange *unchecked* in die Warteschlange *local* verschoben wurden.

Auch diese E-Mail-Nachrichten werden als temporäre Daten behandelt.

Warteschlange "sending"

Die Warteschlange *sending* enthält neue E-Mail-Nachrichten in der Mailwarteschlange, die der SMTP-Service versucht zuzustellen.

Warteschlange "resend"

Die Warteschlange *resend* enthält E-Mail-Nachrichten, die an den SMTP-Zielserver gesendet wurden, aber deren Verarbeitung aufgrund eines temporären Fehlers fehlgeschlagen ist. Temporäre Fehler können unter anderem aus folgenden Problemen resultieren:

- Der SMTP-Server ist nicht erreichbar.
- Der empfangende Mail-Server (ferner Server) gibt einen permanenten Fehler zurück.
- Lotus Protector for Mail Security kann eine E-Mail-Nachricht nicht innerhalb des konfigurierten Intervalls zum erneuten Senden senden.

Eine umfangreiche Warteschlange *resend* zeigt an, dass ein E-Mail-Zustellungsproblem aufgetreten ist.

Warteschlange "frozen"

Die Warteschlange *frozen* enthält E-Mail-Nachrichten, die an den SMTP-Zielserver gesendet wurden, aber deren Verarbeitung aufgrund eines temporären Fehlers fehlgeschlagen ist. Temporäre Fehler können unter anderem aus folgenden Problemen resultieren:

- Der SMTP-Server ist nicht erreichbar.
- Der empfangende Mail-Server (ferner Server) gibt einen permanenten Fehler zurück.
- Lotus Protector for Mail Security kann eine E-Mail-Nachricht nicht innerhalb des konfigurierten Intervalls zum erneuten Senden senden.

Die E-Mail-Nachricht wurde in die Warteschlange *resend* verschoben, damit sie von Lotus Protector for Mail Security erneut gesendet wird. Eine umfangreiche Warteschlange *resend* zeigt an, dass ein E-Mail-Zustellungsproblem aufgetreten ist.

Optional: Verwenden Sie die Option "Erneut spoolen", wenn Sie eine Verzögerung der E-Mail-Nachrichtenverarbeitung feststellen, die einen Rückstand in einem der Spoolverzeichnisse verursacht.

E-Mail-Datenverkehr in den Zustellungswarteschlangen überwachen

Auf der Seite **Warteschlangenbrowser** (SMTP > **Warteschlangenbrowser**) werden die Zustellungswarteschlangen angezeigt, die vom SMTP-Service verwendet werden. E-Mail-Nachrichten warten entweder darauf, analysiert zu werden (*unchecked*), warten auf die Übertragung (*local*, *send*, *resend*), oder es ist eine Fehlerbedingung dafür aufgetreten (*unprocessable*, *frozen*).

Quantitative Erfassung von E-Mail-Nachrichten in einer Warteschlange

Klicken Sie auf den Link [**Anzahl**] neben einer Warteschlange, um die Anzahl der E-Mail-Nachrichten in der Warteschlange anzuzeigen, die noch verarbeitet werden müssen. Klicken Sie auf die Zahl, um die Anzahl der Nachrichten für die Warteschlange zu aktualisieren, ohne dabei die Daten der gesamten Seite aktualisieren zu müssen.

Erneutes Spoolen von E-Mail-Nachrichten

Wenn ein Fehler beim SMTP-Service während der Zustellung einer E-Mail-Nachricht auftritt, wird die Nachricht beim Fehlschlagen eines einzelnen Zustellversuchs in die Warteschlange *resend* verschoben. Wenn alle Zustellversuche fehlschlagen, wird sie in die Warteschlange *frozen* verschoben.

Zustellprobleme können sich ergeben, wenn Lotus Protector for Mail Security oder eine externe Netzkomponente, z. B. der Switch zwischen Lotus Protector for Mail Security und dem SMTP-Zielserver, nicht ordnungsgemäß installiert wurde oder der SMTP-Zielserver selbst nicht verfügbar ist.

Nachdem Sie das Problem behoben haben, kann ein weiterer Zustellversuch durch erneutes Spoolen entweder aller E-Mail-Nachrichten oder bestimmter E-Mail-Nachrichten aus der Warteschlange gestartet werden.

Untersuchen von Warteschlangen

Klicken Sie auf den Namen der Warteschlange, um eine Liste der E-Mail-Nachrichten anzuzeigen, die sich in der Warteschlange befinden, einschließlich der Größe jeder E-Mail-Nachricht sowie des jeweiligen Erstellungsdatums. Jede Seite enthält maximal 1000 Einträge aus der Warteschlange.

Verwenden Sie den Link **Erweitern**, um weitere Dateien in der Warteschlange anzuzeigen. Sie können beispielsweise eine Protokolldatei für E-Mail-Nachrichten anzeigen, die sich in der Warteschlange *resend* oder *frozen* befinden. Diese Protokolldatei enthält Informationen über alle Zustellversuche des SMTP-Service und kann Ihnen nützliche Informationen liefern, um Zustellfehler zu beheben.

Anzeigen von E-Mail-Nachrichten

Klicken Sie auf den Pfad eines Elements in der Warteschlange, um die Inhalte einer E-Mail-Nachricht anzuzeigen.

Eine E-Mail-Nachricht enthält zusätzliche Übermittlungsinformationen am Anfang der angezeigten Daten, während sie sich in einer der Warteschlangen für den SMTP-Service befindet. Abhängig davon, welche Warteschlange Sie anzeigen, können diese Daten durch eine einzelne Leerzeile oder eine Zeile, die `<<MAIL-DATA>>` enthält, von der ursprünglichen E-Mail-Nachricht getrennt sein.

Diese Site zeigt E-Mail-Nachrichten nur als einfachen Text an. Die in HTML geschriebenen Teile der E-Mail-Nachrichten werden nicht verarbeitet.

Anmerkung: Die angezeigten Daten werden bei 4096 Byte abgeschnitten.

Beheben von Zustellungsfehlern

Wenn Warteschlangenprobleme auftreten, versuchen Sie Folgendes:

- Greifen Sie über den Browser für Protokolldateien (**System** > **Protokolldateien**) auf die Protokolldateien zu, um herauszufinden, warum die E-Mail-Nachricht nicht zugestellt wurde.
- Spoolen Sie unverzüglich erneut die markierten E-Mail-Nachrichten sowohl in der Warteschlange *resend* als auch in der Warteschlange *frozen* aus dem SMTP-Warteschlangenbrowser an die SMTP-Warteschlange.
- Löschen Sie E-Mail-Nachrichten aus der Warteschlange *frozen* mithilfe eines Bereinigungsjobs, den Sie auf der Registerkarte "Wartung" auf der Seite "SMTP-Konfiguration" (**SMTP** > **Konfiguration** > **Wartung**) festlegen können.

Kapitel 3. Richtlinienkonfiguration

In diesem Kapitel wird beschrieben, wie Sie eine E-Mail-Sicherheitsrichtlinie konfigurieren können, die Regeln beinhaltet, die definieren, wie Lotus Protector for Mail Security eingehenden und ausgehenden E-Mail-Datenverkehr überprüfen und filtern soll.

Informationen zu Richtlinienregeln

Richtlinienregeln definieren, wie E-Mail-Nachrichten von Lotus Protector for Mail Security untersucht und gefiltert werden sollen, die über das Richtliniensystem weitergeleitet werden.

Bestandteile einer Richtlinienregel

Jede Richtlinienregel besteht aus verschiedenen Objekten (Bedingungsobjekte, Who-Objekte, When-Objekte) und Analysemodulen, die die Analysemethode für E-Mail-Nachrichten von Lotus Protector for Mail Security definieren. Eine Regel besteht außerdem aus Response-Objekten, die das Richtliniensystem anweisen, wie es E-Mail-Nachrichten verarbeiten soll, einschließlich einer Aktion, die dem Richtliniensystem die Vorgehensweise für den Fall vorgibt, dass aus der Regel eine Abgleichsregel wird.

Tabelle 17. Bestandteile einer Richtlinienregel

Option	Beschreibung
Regelname	Gibt den Namen der Richtlinienregel an.
Kommentar	Stellt eine aussagekräftige Beschreibung der Richtlinienregel bereit.
Vorbedingungen	Gibt eine Liste von Bedingungsobjekten an, die die Voraussetzungen zum Bewerten der Richtlinienregel definieren.
Sender	Gibt den Absender einer E-Mail-Nachricht so an, wie er durch den Befehl MAIL FROM während der Übertragung angegeben wird
Empfänger	Gibt den Empfänger einer E-Mail-Nachricht so an, wie er durch den Befehl RCPT TO während der Übertragung angegeben wurde
When-Objekte	Gibt die When-Objekte an, die den Zeitraum definieren, in der die Richtlinienregel gültig ist.
Analysemodule	Stellt eine Liste von Analysemodulen bereit, die eine E-Mail-Nachricht überprüfen können, um die Kategorie ihres Inhalts zu bestimmen
Response-Objekte	Stellt eine Liste von Response-Objekten bereit (konfiguriert auf der Seite "Richtlinienobjekte"), die definieren, wie ein Richtliniensystem eine E-Mail-Nachricht ändern soll, wenn diese mit der Regel übereinstimmt, oder wo die Nachricht gespeichert werden soll
Aktion	Definiert, wie das Richtliniensystem die Verarbeitung einer E-Mail-Nachricht fortsetzen soll, wenn diese mit der Regel übereinstimmt. Die folgenden Aktionen stehen zur Verfügung: • Zulassen: Lässt die Zustellung der E-Mail-Nachricht an ihren Empfänger zu. Damit wird die Verarbeitung der E-Mail-Nachricht durch das Richtliniensystem beendet. • Blockieren: Blockierte E-Mail-Nachrichten werden nicht an ihre Empfänger zugestellt. Damit wird die Verarbeitung der E-Mail-Nachricht durch das Richtliniensystem beendet. • Fortsetzen: Das Richtliniensystem setzt die Verarbeitung der aktuellen E-Mail-Nachricht fort, indem es die nächste Regel in der Kette bewertet.

Verwenden von Regeln im Richtliniensystem

Das Richtliniensystem besteht aus einer Regelkette. Die Regeln werden nacheinander bewertet. Die Reihenfolge verläuft dabei von Anfang bis Ende und von links nach rechts. Wenn eine Regel mehrere Objekte desselben Typs enthält, wird das Ergebnis einer bestimmten Regelkomponente (wie Empfänger oder Analysemodul) als *true* gewertet, wenn mindestens eines der angegebenen Objekte erfolgreich bewertet wurde (logisches ODER).

Das Ergebnis der Bewertung eines Objekts (mit Ausnahme des Response-Objekts) kann immer durch Auswählen der Option **Nicht umschalten** im Popup-Menü eines Objekts zurückgewiesen werden. Dies veranlasst das Richtliniensystem, das Ergebnis der Bewertung eines Objekts umzukehren (das zurückgewiesene Objekt wird als Übereinstimmung gewertet, obwohl das Objekt nicht übereinstimmt).

Das Richtliniensystem verarbeitet die Richtlinie im Kontext eines einzelnen Empfängers. Wenn eine E-Mail-Nachricht mit mehreren Empfängern analysiert wird, bewertet das Richtliniensystem die Regeln gesondert für jeden Empfänger der E-Mail-Nachricht.

Übereinstimmung von Richtlinienregeln

Lotus Protector for Mail Security speichert eine Kopie der ursprünglichen Nachricht, wie sie vom SMTP-Service empfangen wurde, während die aktiven Regeln schrittweise bearbeitet werden. Diese Kopie wird im Richtliniensystem als die *aktuelle Nachricht* bezeichnet, da sie alle Änderungen enthält, die aufgrund vorhergehender Regeln vorgenommen wurden. Wenn die Aktion auf *Zulassen* festgelegt wurde, stellt Lotus Protector for Mail Security die Nachricht an einen bestimmten Empfänger zu. Wenn die Aktion jedoch auf *Blockieren* gesetzt wurde, wird die E-Mail-Nachricht gelöscht (wenn sie nicht zuvor in einer E-Mail-Warteschlange gespeichert wurde).

Lotus Protector for Mail Security führt diese Schritte für jede aktive Richtlinienregel von der ersten bis zur letzten Regel (von Anfang bis Ende) aus, bis eine Regel übereinstimmt und die entsprechende Aktion entweder in *Blockieren* oder *Zulassen* besteht oder aber das Ende der Regelkette erreicht ist (in diesem Fall besteht die Standardaktion in *Zulassen*).

Who-Objekte

Who-Objekte sind einzelne Benutzer oder Benutzergruppen im Richtliniensystem. Who-Objekte können von einer SMTP-Adresse (joe@mycompany.com), SMTP-Adressstrukturen (*@mycompany.com) oder von einem Benutzer oder einer Gruppe aus einem Verzeichnisservice erstellt werden, wie in einem ausgewählten Verzeichnisobjekt definiert.

Typen von Who-Objekten

Tabelle 18. Typen von Who-Objekten

Typ	Beschreibung
E-Mail	Stellt Benutzer oder Gruppen anhand ihrer SMTP-Adresse dar. In der definierten Struktur kann das Platzhalterzeichen * anstelle einer Reihe von Zeichen beliebiger Länge verwendet werden. Sie können die Liste der SMTP-Adressen auch mit Makros wie \$(LOCAL_DOMAINS) füllen. Beispiel: *@mycompany.com
Verzeichnis	Repräsentiert alle dem Verzeichnisservice bekannten Benutzer in dem Verzeichnisobjekt, das von dem Who-Objekt verwendet wird.
Gruppe	Stellt einen bestimmten Typ eines Verzeichnisobjekts dar. Eine Übereinstimmung ist nur dann gegeben, wenn der Benutzer, der eine bestimmte SMTP-Adresse verwendet, Mitglied der angegebenen Gruppe in dem Verzeichnis ist, das von dem ausgewählten Verzeichnisobjekt verwendet wird. Der Name der Gruppe im Who-Objekt entspricht dem Namen im Verzeichnis.
Benutzer	Stellt einen einzelnen Benutzer anhand seines Namens in einem Verzeichnis dar. Die SMTP-Adresse dieses Benutzers wird durch das Namensattribut aufgelöst, das für das verwendete Verzeichnisobjekt konfiguriert ist.
Verbund, Who	Kombiniert verschiedene Typen von Who-Objekten (wie zuvor angeführt) in einem einzelnen Objekt. Ein Verbund-Who-Objekt stimmt überein, wenn eines der Who-Objekte in dem Verbund von Who-Objekten übereinstimmt.

Überprüfen von Empfängern mit Who-Objekten

Who-Objekte werden nicht nur für die Regeln der Richtlinie verwendet, sondern ebenso, um das Vorhandensein eines Benutzers in Ihrer Umgebung bei der Zustellung einer E-Mail-Nachricht zu überprüfen. Der Mechanismus zur Empfängerüberprüfung ist in den SMTP-Service integriert, der E-Mail-Nachrichten an unbekannte Empfänger auf SMTP-Ebene zurückweist. Dieser Mechanismus verwendet die gleichen Who-Objekte, die von Ihnen in den Richtlinienregeln verwendet werden.

Who-Objekte überprüfen

Auf der Seite **Who-Objekte überprüfen** (**Mail Security > Who-Objekte überprüfen**) können Sie überprüfen, ob (insbesondere verzeichnisbasierte) Who-Objekte ordnungsgemäß konfiguriert wurden.

Auf dieser Seite werden zwei verschiedene Methoden zum Überprüfen von Who-Objekten vorgestellt. Mit der Methode "Alle Who-Objekte" können Sie überprüfen, ob alle Who-Objekte (einschließlich zugrunde liegender Verzeichnisobjekte) ordnungsgemäß konfiguriert wurden. Wenn Sie überprüfen möchten, ob eine bestimmte E-Mail-Adresse mit mindestens einem Who-Objekt übereinstimmt, wählen Sie eine SMTP-Adresse aus der Liste aus.

Tabelle 19. Who-Objekte überprüfen

Option	Beschreibung
Who	Gibt den Namen des Who-Objekts gemäß der Konfiguration auf der Seite Mail Security-Richtlinienobjekte an.
Typ	Gibt den Typ des Who-Objekts an: • E-Mail-Muster: Repräsentiert Benutzer oder Gruppen durch ihre SMTP-Adresse • Verzeichnis: Stellt alle durch den Verzeichnisservice bekannten Benutzer in dem Verzeichnisobjekt dar, das von dem Who-Objekt verwendet wird. • Gruppe: Stellt einen bestimmten Typ eines Verzeichnisobjekts dar. Eine Übereinstimmung ist nur dann gegeben, wenn der Benutzer, der eine bestimmte SMTP-Adresse verwendet, Mitglied der angegebenen Gruppe in dem Verzeichnis ist, das von dem ausgewählten Verzeichnisobjekt verwendet wird. Der Name der Gruppe im Who-Objekt entspricht dem Namen im Verzeichnis. • Benutzer: Stellt einen einzelnen Benutzer anhand seines Namens in einem Verzeichnis dar. Die SMTP-Adresse dieses Benutzers wird durch das Namensattribut aufgelöst, das für das verwendete Verzeichnisobjekt konfiguriert ist. • Verbund Who: Kombiniert mehrere unterschiedliche Typen von Who-Objekten (wie oben erwähnt) in ein einzelnes Objekt. Ein Verbund-Who-Objekt stimmt überein, wenn eines der Who-Objekte in dem Verbund von Who-Objekten übereinstimmt.
Beschreibung	Gibt eine Beschreibung dessen an, was vom Who-Objekt dargestellt wird.
SMTP-Abgleich	Gibt an, ob die angegebene E-Mail-Adresse mit dem angegebenen Who-Objekt übereinstimmt
Nur SMTP-Adresse	
Ergebnis	Gibt an, ob Lotus Protector for Mail Security die Informationen vom angegebenen Who-Objekt oder vom zugrunde liegenden Verzeichnisobjekt abrufen konnte. Wenn das angegebene Who-Objekt ein Verzeichnisobjekt verwendet, können Sie detaillierte Informationen über die abgerufenen Daten erhalten oder Sie können herausfinden, warum die Suche fehlgeschlagen ist, indem Sie auf den Wert in dieser Spalte klicken.

When-Objekte

When-Objekte definieren bestimmte Zeitrahmen, z. B. Bürozeiten. Sie verwenden diese Objekte innerhalb des Richtliniensystems, um anzugeben, wann eine Regel gültig ist, die ein When-Objekt enthält.

Vorgehensweise

1. Klicken Sie im Navigationsfenster auf **Mail Security > Richtlinienobjekte**.
2. Klicken Sie auf die Registerkarte **When** und anschließend auf **Hinzufügen**.
3. Aktivieren Sie das Kontrollkästchen **Aktiv**.
4. Geben Sie einen Namen für das When-Objekt ein.
5. Klicken Sie im Bereich **Zeitraum** auf **Hinzufügen**.
6. Legen Sie die folgenden Werte fest:

Option	Bezeichnung
Zeit	Gibt die Startzeit des Zeitrahmens an, der durch das When-Objekt definiert wird. Anmerkung: Bei dem für ein neues When-Objekt automatisch eingegebenen Datum handelt es sich um die Zeit des Systems, auf dem Lotus Protector Manager ausgeführt wird, und nicht um die aktuelle Systemzeit von Lotus Protector for Mail Security. Die Startzeit kann aber auch der Zeitzone Ihres Web-Browsers oder der Greenwich Mean Time (GMT, Westeuropäische Zeit) entsprechen.
Dauer	Gibt den Umfang des Zeitrahmens an, der durch dieses When-Objekt definiert wird.
Wiederholen alle	Legt die Zeitspanne zwischen jeder Wiederholung fest, beginnend mit der Startzeit.

Beispiel: Legen Sie ein When-Objekt fest, um die Anzahl der eingehenden E-Mail-Nachrichten zwischen zwei Empfängern zu verteilen, wobei Zeitintervalle von 5 Minuten verwendet werden:

Start: 2009-06-15 00:00:00 GMT, Dauer: 5 Minuten, Wiederholung alle 10 Minuten

wobei der Wert der Start-**Zeit** für das neue When-Objekt der 15. Juni 2009 00:00:00 GMT ist, der Wert für die **Dauer** auf 5 Minuten festgelegt ist und der Wert für **Wiederholen alle** auf 10 Minuten festgelegt ist.

7. Klicken Sie auf **OK** und anschließend auf **Änderungen speichern**.

Bedingungsobjekte

Bedingungsobjekte bilden die Voraussetzung dafür, unter welchen Umständen eine Richtlinienregel auf eine eingehende E-Mail-Nachricht zutrifft. Diese Bedingungen werden für jede E-Mail-Nachricht, die von Lotus Protector for Mail Security verarbeitet wird, separat bewertet und geändert.

Eine Bedingung speichert die Ergebnisse einer Richtlinienregel ab (ob die Richtlinienregel zutraf oder nicht), die Sie anschließend als Kriterien für andere Richtlinienregeln verwenden können. Der Anfangswert einer Bedingung ist immer *false*.

Sie können Ihre Richtlinienregeln mithilfe der Bedingungen optimieren. Sie können eine Bedingung erstellen, die das Auswerten bestimmter Richtlinienregeln verhindert, wenn eine E-Mail-Nachricht nicht den in einer vorherigen Richtlinienregel definierten Kriterien entsprach, oder Sie können eine Bedingung erstellen, die die Richtlinienregeln nur dann auswertet, wenn die E-Mail-Nachricht nicht den definierten Kriterien entspricht. Wenn Sie mehrere Richtlinienregeln mit gemeinsamen Kriterien verwenden, empfiehlt sich die Verwendung von Bedingungen.

Tabelle 20. Bedingungsobjekte

Option	Beschreibung
Name	Gibt den Namen eines Bedingungsobjekts an, das in einem Richtliniensystem verwendet wird.
Kommentar	Beinhaltet die Beschreibung eines Bedingungsobjekts.

Bedingungsobjekte verwenden (Beispiel)

Wenn Sie den E-Mail-Datenverkehr für einen bestimmten Empfänger (oder eine Empfängergruppe) verwalten möchten, indem Sie eine E-Mail-Nachricht mit einem bestimmten Schlüsselwort im Betreff verfolgen, können Sie im Richtliniensystem eine Regel definieren, die ein Who-Objekt, das die Empfänger darstellt, sowie ein Analysemodul enthält, mit dem überprüft wird, ob das Schlüsselwort im Betreff enthalten ist. Sie müssen eine Response für diese Art von E-Mail-Nachrichten mithilfe eines Response-Objekts definieren, mit dem der Wert der Bedingung auf *true* festgelegt wird.

Mit der folgenden Regel können Sie überprüfen, ob eine E-Mail-Nachricht den angegebenen Kriterien entspricht, indem Sie das Bedingungsobjekt der Liste der Vorbedingungen hinzufügen. Empfänger sind beispielsweise nicht berechtigt, E-Mail-Nachrichten zu empfangen, die ausführbare Dateien enthalten. Außerdem sollten alle Spam-E-Mail-Nachrichten in einem bestimmten Nachrichtenspeicher für diese Empfänger gespeichert werden. Sie müssen eine Regel erstellen, die den Wert des Bedingungsobjekts testet; fügen Sie zudem einen neuen Dateityp für das Analysemodell hinzu (Typ: Anwendung) und legen Sie *Blockieren* als Aktion fest. Ferner legen Sie eine weitere Regel fest, mit der auch der Wert des Bedingungsobjekts überprüft wird und die eine Reihe von Analysemodulen zur Spamerkennung mit einer entsprechenden Response zum Speichern von E-Mail-Nachrichten in einem bestimmten Nachrichtenspeicher verwendet.

Analysemodule

Lotus Protector for Mail Security verwendet verschiedene Spamanalysemodule, um den Inhalt von E-Mail-Nachrichten zu überprüfen.

Anhangprüfung

Dieses Modul analysiert die Anzahl der Anhänge, die Größe einzelner Anhänge oder die Größe aller Anhänge. Sie können diese Funktion beispielsweise verwenden, wenn Sie Probleme mit der Bandbreite haben und die Zustellung von E-Mail-Nachrichten mit großen Anhängen verzögern möchten.

Verbund

Dieses Modul besteht aus einer Kombination mehrerer Analysemodule. Sie können den einzelnen Modulen unterschiedliche Punktzahlen zuweisen und einen Schwellenwert definieren.

Schlüsselwortsuche

Dieses Modul stellt eine Suchmaschine für reguläre Ausdrücke dar. Mit diesem Modul können Sie Ihre eigenen Kategorien erstellen, die Konformitätsprüfungen durchführen.

Sprachprüfung

Dieses Modul wird verwendet, wenn Sie Lotus Protector for Mail Security trainieren, E-Mail-Nachrichten aus anderen Ländern als den Vereinigten Staaten zu analysieren. Lotus Protector for Mail Security unterstützt derzeit mehr als 40 verschiedene Sprachen. Es ist möglich, E-Mail-Nachrichten zu blockieren oder umzuleiten, die in einer Sprache verfasst sind, die der Mitarbeiter nicht lesen kann.

Dateityp

Dieses Modul erkennt mehr als 120 verschiedene Dateitypen. Sie können dadurch beispielsweise gefährliche Dateitypen wie ausführbare Programme löschen.

Nachrichtenfeldprüfung

Mit diesem Modul können Sie mithilfe von regulären Ausdrücken nach bestimmten Ausdrücken innerhalb des Nachrichtenfelds einer E-Mail-Nachricht suchen. Sie können diese Funktion beispielsweise verwenden, um nach bestimmten Wörtern im Betreff der E-Mail zu suchen oder um HTML-E-Mail-Nachrichten zu identifizieren (Prüfung des Inhaltstyps des Headerfelds).

Phishing-Prüfung

Phishing-E-Mail-Nachrichten sind Spamnachrichten, die persönliche Informationen von potenziellen Opfern abrufen sollen. Üblicherweise sehen Phishing-E-Mail-Nachrichten ähnlich aus wie Nachrichten von bestimmten Banken oder Einkaufswebsites. Mithilfe dieser Nachrichten sollen die Konteninformationen des Empfängers einschließlich der Kennwörter ausfindig gemacht werden. In den meisten Fällen ist es für den durchschnittlichen Benutzer sehr schwierig, eine Phishing-E-Mail-Nachricht von einer echten E-Mail-Nachricht, die von der eigenen Bank verschickt wurde, zu unterscheiden.

Um Phishing erkennbar zu machen, kombiniert IBM eine Vielzahl von Methoden. Das URL-Prüfprogramm kann Links auf Banking- und andere kommerzielle Sites in Spamnachrichten erkennen, die aus den Spam-Collectors kommen. Phishing-E-Mail-Nachrichten weisen außerdem im Vergleich zu anderen Spamnachrichten eine typische Heuristik auf. Sie werden in der Filterdatenbank gesondert kategorisiert.

Sender Policy Framework

Wichtig: Wenn Sie den Headertyp für Empfang mit **Eingeschränkt (keine IP wird angezeigt)** angeben und dann Ports in Ihrer Firewall für den Empfang von SMTP-Datenverkehr öffnen, funktionieren die Analysemodule des Sender Policy Framework nicht, da diese Module auf Informationen im empfangenen Header angewiesen sind.

Das Modul für das Sender Policy Framework wertet einen SPF-Eintrag aus und produziert eines der folgenden Ergebnisse:

Tabelle 21. Ergebnisse des Sender Policy Frameworks

Ergebnis	Beschreibung
Keins	Die Domäne veröffentlicht keine SPF-Daten.
Neutral	Der SPF-Client muss so fortfahren, als ob eine Domäne keine SPF-Daten veröffentlicht hat. Dieses Ergebnis wird ausgegeben, wenn der SPF-Eintrag den Befehl "?all" angibt.
Bestanden	Die E-Mail-Nachricht erfüllt die Definition der Zulässigkeit für die veröffentlichende Domäne. Die Nachrichtenübertragungsagenten wenden daraufhin die lokale Richtlinie an und können die E-Mail-Nachricht entsprechend annehmen oder zurückweisen.
Nicht bestanden	Die E-Mail-Nachricht entspricht nicht der Definition der Zulässigkeit für eine Domäne. Die Nachrichtenübertragungsagenten weisen die E-Mail-Nachricht möglicherweise mit einem Antwortcode für einen permanenten Fehler zurück, z. B. mit Code 550.
Leicht fehlgeschlagen	Die E-Mail-Nachricht entspricht nicht der strengen Definition für die Zulässigkeit für eine Domäne, aber die Domäne kann nicht sicher feststellen, dass es sich bei der E-Mail-Nachricht um einen Betrugsversuch handelt. Die Nachrichtenübertragungsagenten nehmen die E-Mail-Nachricht normalerweise an, schreiben jedoch möglicherweise höhere Transaktionskosten oder eine ausführlichere Prüfung vor oder vergeben eine ungünstige Bewertung. Es existieren zwei Fehlerbedingungen, eine vorläufige und eine permanente.
Fehler	Verweist auf einen Fehler bei der Suche. Nachrichtenübertragungsagenten weisen die E-Mail-Nachricht üblicherweise mit einem temporären Fehlercode zurück, z. B. 450.
Unbekannt	Zeigt eine unvollständige Verarbeitung an; ein MTA fährt so mit der Verarbeitung fort, als ob die Domäne keine SPF-Daten veröffentlicht hat. Wenn SPF-fähige SMTP-Empfänger eine E-Mail-Nachricht akzeptieren, sollten sie ein Präfix zum SPF-Empfangsheader hinzufügen. SPF-Clients müssen den in diesem Abschnitt beschriebenen Algorithmus oder sein funktionales Äquivalent verwenden. Wenn ein SPF-Client einen Syntaxfehler in einem SPF-Eintrag feststellt, muss er die Verarbeitung unterbrechen und ein Ergebnis "Unbekannt" zurückgeben.

Spam-Bayes-Klassifikator

Der Bayes-Klassifikator ist ein System, das anhand von E-Mail-Statistikdaten überprüft, ob es sich bei einer E-Mail-Nachricht um Spam handelt.

Um den Klassifikator zu trainieren, werden dem System Tausende von Spambeispielen und regulären E-Mail-Nachrichten vorgelegt. Dabei werden wichtige Daten extrahiert und in einem statistischen Modell gespeichert. Durch dieses Training kann der Klassifikator die Unterscheidung zwischen Spammnachrichten und regulären E-Mail-Nachrichten erlernen.

IBM stellt eine aktualisierte und vorbereitete Bayes-Datenbank bereit, die unter Verwendung von Tausenden von unterschiedlichen Spamtypen aus den Spam-Collectors und mithilfe von Benutzer-Feedback initi-

alisiert wurde. Sie können eine Feinabstimmung der Filter vornehmen oder einen völlig neuen Filter sensibilisieren, indem Sie ihm zusätzliche Beispiele für Spam und zuführen.

Der Vorteil eines bayesschen Klassifikationsmerkmals liegt in seiner Fähigkeit, neue Spamtypen zu erkennen, wogegen die Stärken der Signaturtechnologie in der Erkennung identischen und nahezu identischen Spams liegen.

Spam-DNSBL-Prüfung

Dieses Modul verwendet DNSBL-Server (Domain Name Server Block Lists-Server), um zu ermitteln, ob E-Mail-Nachrichten einer möglichen Spamquelle entspringen. Sie können mehrere Server mit entsprechenden Bewertungen verwenden, um eine präzisere Erkennung zu generieren, die mit einer höheren Flexibilität einhergeht.

Spamfingerabdruck

Für jede E-Mail-Nachricht wird eine eindeutige, 128-stellige Signatur berechnet. Verwenden Sie die Signaturen in der Filterdatenbank, um bestehende Spamnachrichten zu identifizieren.

Lotus Protector for Mail Security berechnet Spamsignaturen für alle bekannten Spams (von Spam-Collectors und anderen Quellen) und speichert die Signaturen in der Filterdatenbank.

Spamdatenflussprüfung

Dieses Modul analysiert den E-Mail-Datenfluss innerhalb eines bestimmten Zeitrahmens. Wenn die gleiche E-Mail-Nachricht (ermittelt anhand von Ähnlichkeitskriterien) innerhalb des Zeitrahmens häufiger als durch den Schwellenwert festgelegt empfangen wird und verschiedene Senderdomänen hat, wird die E-Mail-Nachricht als Spam klassifiziert. Mithilfe dieser Technologie können auf Basis der Art und Weise, wie Spam typischerweise erstellt und versendet wird, völlig unbekannte Spamtypen erkannt werden.

Spamheuristik

Dieses Modul verwendet ein internes Scoring-System, bei dem jede Heuristik entweder positive oder negative Punkte erhält, abhängig davon, ob die Heuristik Spamnachrichten oder erwünschte E-Mails (HAM) abgleichen soll. Falls der Punktezähler einen vordefinierten Schwellenwert erreicht, wird die E-Mail-Nachricht als Spam klassifiziert.

Die folgenden Informationen werden z. B. für die heuristische Analyse verwendet:

- Feldmerkmale der Nachrichten-ID
- Das empfangene Feld ist nicht gültig oder fehlt
- Überprüft, ob die Felder "Apparently-To:" oder "X-Apparently-To:" vorhanden sind
- Überprüft, ob Mailing-Listenfelder vorhanden sind
- Überprüft, ob mehrere Empfänger und alphabetische Empfängermuster wie a@, b@, c@ vorhanden sind
- Überprüft, ob Felder wie "From" und "To" fehlen

Spamschlüsselwort

Dieses Modul berücksichtigt Standardschlüsselwörter und -muster (reguläre Ausdrücke), die in Spam-E-Mail-Nachrichten üblicherweise gefunden werden.

IBM hat entsprechende Schlüsselwörter und Muster aus bekannten Spamnachrichten extrahiert und ihre jeweilige Relevanz für einen zusätzlichen Spamschutz gewichtet.

Spamsignaturdatenbank

Mit diesem Modul kann Lotus Protector for Mail Security jede E-Mail-Nachricht in mehrere logische Teile unterteilen (Sätze, Absätze) und eine eindeutige, 128-stellige Signatur für jeden Teil errechnen. Diese Signaturen können in der E-Mail-Nachricht leicht verändert sein, sind jedoch präzise genug, um eine bekannte Spamnachricht mit mehreren übereinstimmenden Signaturen in der Filterdatenbank zu identifizieren.

Spamstrukturprüfung

Dieses Modul überprüft die HTML-Struktur der E-Mail-Nachricht und errechnet zwei Signaturen anhand der Struktur.

So verfügen manche Spamnachrichten z. B. über eine fette Überschrift gefolgt von einem oder mehreren Absätzen in unterschiedlicher Farbe sowie etwas Zufallstext im unteren Bereich. Layoutstrukturen dieser Art ähneln dem tatsächlichen Text in der E-Mail-Nachricht und sind daher eine gute Ergänzung zu den oben beschriebenen textuellen Spamsignaturen.

Das Modul berechnet Struktursignaturen für den gesamten bekannten Spam (aus Spam-Collectors und anderen Quellen) und speichert sie und die URLs in der Filterdatenbank.

Spam-URL-Prüfung

Dieses Modul vergleicht Daten mit den im Internet gefundenen URL-Einträgen. Alle relevanten URLs, die in Spam-E-Mail-Nachrichten auftauchen, werden in der Filterdatenbank zusammen mit den gespeicherten Spamsignaturen gespeichert. Eine einzige Spam-URL reicht aus, um eine Spam-E-Mail-Nachricht zu identifizieren.

URL-Prüfung

Dieses Modul analysiert URLs in E-Mail-Nachrichten mithilfe von Inhalten aus der Filterdatenbank. Lotus Protector for Mail Security bietet mehr als 61 Kategorien, mit denen Sie E-Mail-Nachrichten mit unerwünschten oder gefährlichen Links blockieren können.

Absenderzulassungsliste für Benutzer

Jeder Benutzer kann eine eigene Zulassungsliste für Absender verwalten. Sie können genau angeben, welcher Benutzer diese Funktion nutzen darf und an welcher Stelle in der Regelkette diese Überprüfung ausgeführt werden soll.

Absenderblockierliste für Benutzer

Jeder Benutzer kann seine eigene Absenderblockierliste verwalten. Sie können genau angeben, welcher Benutzer diese Funktion nutzen darf und an welcher Stelle in der Regelkette diese Überprüfung ausgeführt werden soll.

Virenprüfung

Dieses Modul bietet zwei Module, die Antivirensoftware verwenden, um Viren zu ermitteln und infizierte E-Mail-Nachrichten zu verarbeiten:

- Signaturmustererkennung
- Malware-Fernerkennung

Sie können zwischen einem musterbasierten Scanner, wie z. B. Sophos (wenn Sie eine gültige Lizenz installiert haben), und dem Malware-Fernerkennungsscanner wählen.

Spamanalysemodule verwenden

Dieser Abschnitt beschreibt die Vorgehensweise bei der Aktivierung der Spamanalysemodule, die verwendet werden, um den Inhalt einer E-Mail-Nachricht zu überprüfen.

Vorgehensweise

1. Klicken Sie im Navigationsfenster auf **Mail Security > Richtlinienobjekte**.
2. Klicken Sie auf die Registerkarte **Analysemodul** und anschließend auf **Hinzufügen**.
3. Aktivieren Sie das Kontrollkästchen **Aktiviert**, um die Regel zu aktivieren.
4. Geben Sie einen Namen und einen Begleittext für die Regel ein.
5. Wählen Sie ein Spamanalysemodul aus. Siehe „Analysemodule“ auf Seite 53 für eine detaillierte Beschreibung für jedes Modul.
6. Klicken Sie auf **OK** und anschließend auf **Änderungen speichern**.

Response-Objekte

Response-Objekte definieren, wie eine E-Mail-Nachricht nach der Analyse durch Lotus Protector for Mail Security weiter verarbeitet werden soll.

Tabelle 22. Typen von Response-Objekten

Option	Beschreibung
Anhang hinzufügen	Stellt eine Response bereit, die den Inhalt oder die Art einer ursprünglichen Nachricht ändert, indem ein hinzugefügter Anhang verwendet wird, der die aktuelle E-Mail-Nachricht, die ursprüngliche E-Mail-Nachricht oder eine Datei enthält
Haftungsausschluss hinzufügen	Stellt eine Response bereit, die den Inhalt oder die Art einer ursprünglichen E-Mail-Nachricht ändert, indem ein standardmäßiger Haftungsausschluss des Unternehmens jeder ausgehenden E-Mail angehängt wird
BCC	Sendet eine Kopie der E-Mail-Nachricht als Blindkopie an den angegebenen Empfänger Sie können die als BCC versendete E-Mail-Nachricht mit anderen Aktionsobjekten modifizieren. Die BCC-Aktion wird auf alle E-Mail-Nachrichten angewendet, ob zugelassen oder blockiert. • \$(SENDER): Die für die ursprüngliche E-Mail-Adresse verwendete Absenderadresse • \$(RECIPIENTS): Eine Liste aller Empfänger der ursprünglichen E-Mail-Nachricht • \$(ALLOWEDRCPTS): Eine Liste aller Empfänger, die zugelassen wurden • \$(BLOCKEDRCPTS): Eine Liste aller Empfänger, die blockiert wurden • \$(NEWMSGSENDER): Die für neu erstellte E-Mail-Nachrichten verwendete Absenderadresse • \$(POSTMASTER): Sendet die ermittelte E-Mail-Adresse an den ursprünglichen Absender als postmaster@mycompany.com und informiert den Absender darüber, dass die ursprüngliche E-Mail-Nachricht unter Quarantäne gestellt wurde
Protokoll	Schreibt in eine unverschlüsselte Textdatei (mit ersetzten Makros), schreibt aber nicht in die Lotus Protector for Mail Security-Datenbank.
Felder ändern	Ändert ein Feld oder fügt ein Feld im Header einer E-Mail-Nachricht hinzu Wichtig: Seien Sie besonders vorsichtig, wenn Sie Nachrichtenfelder modifizieren. Modifizieren Sie keine Felder, die Ihre E-Mail-Nachricht beschädigen und somit verursachen können, dass die E-Mail-Nachricht gelöscht wird, statt ihren Empfänger zu erreichen.

Tabelle 22. Typen von Response-Objekten (Forts.)

Option	Beschreibung
Umleiten	Sendet die E-Mail-Adresse an den angegebenen Empfänger • \$(SENDER): Die für die ursprüngliche E-Mail-Adresse verwendete Absenderadresse • \$(RECIPIENTS): Eine Liste aller Empfänger der ursprünglichen E-Mail-Nachricht • \$(ALLOWEDRCPTS): Eine Liste mit allen Empfängern, die zugelassen wurden • \$(BLOCKEDRCPTS): Eine Liste mit allen Empfängern, die blockiert wurden • \$(NEWMSGSENDER): Die für neu erstellte E-Mail-Nachrichten verwendete Absenderadresse • \$(POSTMASTER): Sendet die ermittelte E-Mail-Adresse an den ursprünglichen Absender als postmaster@mycompany.com und informiert den Absender darüber, dass die ursprüngliche E-Mail-Nachricht unter Quarantäne gestellt wurde
Weiterzugebende Nachricht	Leitet eine bestimmte E-Mail-Adresse an einen bestimmten Host weiter
Anhang löschen	Analysiert in der E-Mail-Nachricht gefundene Anhänge Wenn der Anhang den Bedingungen Who/When/What entspricht, entfernt Lotus Protector for Mail Security den Anhang (oder alle Anhänge) aus der ursprünglichen E-Mail-Nachricht. Anmerkung: Wenn Sie diese Aktion verwenden, um einen uu-codierten Textblock zu löschen und die Option "Anhänge abgleichen" auswählen, werden weitere uu-codierte Teile der E-Mail-Nachricht in der entstehenden E-Mail-Nachricht als Anhänge eingetragen.
Verschlüsselung erforderlich	Ermöglicht dem Administrator, eine Response zu konfigurieren, durch die eine E-Mail-Nachricht, die mit bestimmten Regeln übereinstimmt, mit TLS (Transport Layer Security) zugestellt werden muss • Wenn Sie E-Mail-Nachrichten an eine bestimmte Domäne mit Verschlüsselung senden möchten, erstellen Sie eine Richtlinienregel mit einer Response "Verschlüsselung erforderlich" von My domains an this.specific.domain. • Wenn es für das Versenden von E-Mail-Nachrichten erforderlich ist, dass alle E-Mail-Nachrichten, die einen unternehmensvertraulichen Haftungsausschluss verwenden, mit Verschlüsselung versendet werden, erstellen Sie eine Richtlinienregel von Eigene Domänen, für den Fall, dass die E-Mail-Nachricht "unternehmensvertraulich" und eine Response "Verschlüsselung erforderlich" enthält. Anmerkung: Wenn eine E-Mail-Nachricht als TLS-Zustellung markiert ist, das SMTP-Gegenstück aber kein TLS unterstützt, versucht das System, die E-Mail-Nachricht als "normal" konfigurierten SMTP-Verkehr erneut zu senden, indem es Unzustellbarkeitsberichte an den Absender sendet. Wenn die E-Mail-Nachricht allerdings nicht per TLS zugestellt werden kann, wird das System sie auch nicht zustellen.
Senden an	Fordern Sie die Anwendung auf, dem Absender der analysierten E-Mail-Nachricht oder einer anderen Person (z. B. dem Administrator) zu antworten und verwenden Sie verschiedene Optionen zur Änderung des Inhalts der E-Mail-Adresse. Mit diesem Objekt können Sie die folgenden Aktionen ausführen: • Eine neue E-Mail-Nachricht an den Sender erstellen • Einen Anhang hinzufügen • Die ursprüngliche E-Mail-Nachricht als Anhang hinzufügen • Eine vordefinierte Warnungs-E-Mail-Nachricht an den ursprünglichen Absender senden
Bedingung für Einstellen/Löschen	Legt den Zustand einer Bedingung (oder eines Schalters) fest, die verwendet wird, um bestimmte Regeln in der Richtlinie dynamisch zu aktivieren oder zu deaktivieren.
Geschäft	Sendet die E-Mail-Nachricht an einen Sammelordner. Sie können ebenso auswählen, ob die ursprüngliche oder die aktuelle E-Mail-Nachricht (E-Mail-Nachricht, die von einer anderen Richtlinienregel geändert wurde) gespeichert werden soll.

Verzeichnisobjekte

Dieser Abschnitt beschreibt, wie Lotus Protector for Mail Security mit einem Verzeichnisobjekt, z. B. einem LDAP-Verzeichnisservice (Lightweight Directory Access Protocol-Verzeichnisservice), integriert werden kann und wo Sie auf die Benutzerdatenbank Ihres Verzeichnisservice zugreifen und sie zusammen mit Who-Objekten und Richtlinienregeln verwenden können.

LDAP-Verzeichnissever

Ein LDAP-Server ist ein Verzeichnisservice, z. B. Active Directory, IBM Lotus Domino Directory, OpenLDAP, Novell eDirectory, Oracle Internet Directory, Sun ONE, der Informationen über Menschen, Unternehmen und andere Ressourcen speichert und auf den über das LDAP-Protokoll zugegriffen wird. Die Einträge in dem Verzeichnis sind in einer hierarchischen Struktur angeordnet, wobei die hierarchische Struktur in einigen Fällen die Hierarchie oder Struktur eines Unternehmens widerspiegelt.

LDAP-Verzeichnissever stellen Benutzer- und Benutzer-/Gruppeninformationen für Lotus Protector for Mail Security bereit. Sie können die Konfiguration von Who-Objekten vereinfachen, indem Sie die vom LDAP-Server bereitgestellten Benutzernamen und Gruppen den Who-Objekten zuordnen, die Sie für eine Richtlinie definieren.

Tipp: Wenn Sie die Struktur Ihres Verzeichnisservice nicht genau kennen, können Sie mithilfe des Verzeichnisservice-Browsers (z. B. LDAP-Browser/-Editor nach Jarek Gawor) Ihr Verzeichnis durchsuchen oder bearbeiten.

Einstellungen für Verzeichnisobjekte

Geben Sie die Einstellungen für einen Verzeichnisservice an, die das Verzeichnisobjekt definieren:

Option	Beschreibung
Name	Der Name des Verzeichnisobjekts, das den Verzeichnisservice im Richtliniensystem repräsentiert.
Kommentar	Optionaler Kommentar für den Verzeichnisservice.
Ablauf des Cachespeichers	Die Zeit, für die Lotus Protector for Mail Security Benutzer- und Gruppeninformationen lokal speichert. Lotus Protector for Mail Security fragt den Verzeichnisservice nicht ab, wenn Informationen, die in seinem Verzeichniscache gefunden wurden, seine Leistung verbessern. Stellen Sie sicher, dass Sie einen geeigneten Ablaufwert einstellen, da zwischengespeicherte Daten nicht zwingend die letzten Änderungen für das Verzeichnis beinhalten. Standard: Stellen Sie den Standardwert von 1440 Minuten (1 Tag) als Kompromiss zwischen Leistung und Aktualität ein.

Einstellungen für den LDAP-Server

Option	Beschreibung
Host	Der Name des Hosts oder die IP-Adresse des Verzeichnisserviceanbieters.
Port	Der Port, auf dem der Verzeichnisservice für eingehende Verbindungen empfangsbereit ist. Standard: Port 389 für unverschlüsselte Anforderungen; Port 636 für SSL-Anfragen
Benutzername	Der Benutzername eines Verzeichnisbenutzers, der den Verzeichnisservice auflisten darf. Anmerkung: Das Format für diesen Accountnamen hängt davon ab, welchen Verzeichnisservice Sie verwenden. Active Directory verwendet z. B. mycorp\administrator. Andere Software verwendet möglicherweise andere Namen wie z. B. cn=Directory Manager,o=mycorp.
Kennwort	Das Kennwort für den Benutzer, das in das Benutzernamensfeld eingegeben wird.

Option	Beschreibung
OU (Verzeichnisein- tragspunkt)	Der Verzeichniseintragspunkt (BaseDN) für die Verzeichnissuche. Format: DC=domain,DC=com
Modus	• Basis: Verwendet den an der OU (Verzeichniseintragspunkt) konfigurierten Eintrag. • Eine Ebene: Verwendet nur die Einträge, die sich direkt im Basis-DN befinden, der an der OU (Verzeichniseintragspunkt) konfiguriert wurde. • Unterverzeichnisstruktur: Verwendet den Basis-DN, der an der OU (Verzeichniseintragspunkt) konfiguriert wurde, sowie alle Einträge, die sich unterhalb dieses Eintrags in der Verzeichnisinformationsbaumstruktur befinden.
ObjectClass oder ObjectCategory verwenden	• ObjectClass: Verwendet ObjectClass-Attribute, um den Typ des Verzeichniseintrags zu bestimmen. • ObjectCategory: Verwendet bestimmte Verzeichniseinträge innerhalb eines Active Directory. Dieses Attribut wird ebenso wie das ObjectClass Attribut bei der Bestimmung des Typs eines Eintrags verwendet. Allerdings bestehen folgende Unterschiede: – Pro Verzeichniseintrag existiert nur ein Attribut mit dem Namen ObjectCategory. – Dieses Attribut wird typischerweise in der zugrunde liegenden Datenbank auf dem Server indexiert. Tip: Verwenden Sie ObjectCategory statt ObjectClass, um die Leistung auf großen Domänen oder langsamen Servern zu verbessern, wenn Sie Active Directory verwenden.

Benutzereinstellungen

Option	Beschreibung
Objektklassen	Definiert den Wert eines Attributs für ObjectClass, das einen Verzeichniseintrag als einen Benutzer identifiziert. In den meisten Fällen wird dieser Eintrag auf <i>Person</i> eingestellt.
Namensattribut	Gibt den Namen des Attributs eines Verzeichnisbenutzers an, das die Anmeldedaten oder den Kurznamen des Benutzers enthält. Anmerkung: Je nachdem, wie Sie Who-Objekte für die Richtlinienregeln und die Authentifizierung mit der Endbenutzerschnittstelle konfigurieren, können Sie entweder den Anmeldenamen oder den tatsächlichen Namen des Benutzers verwenden.

Gruppeneinstellungen

Option	Beschreibung
Objektklasse	Definiert den Wert des Attributs für ObjectClass, das einen Verzeichniseintrag als eine Gruppe identifiziert. Dieser Wert kann je nach dem, welchen Gruppentyp Sie auswählen und je nach Struktur Ihres Verzeichnisservice variieren. Allgemeine Werte sind Gruppe, Unternehmen oder Land.
Namensattribut	Gibt den Namen eines Attributs für eine Verzeichnisgruppe an, das den Namen der Gruppe enthält.

Mitgliedereinstellungen

Option	Beschreibung
Mitgliedschaft definiert in	Wählen Sie die Methode aus, die verwendet werden soll, um die Gruppen zu ermitteln, denen ein bestimmter Benutzer oder eine bestimmte Gruppe angehört: • Mitgliedsobjekt: Das Objekt selbst, also entweder ein Benutzer oder eine Gruppe, das eine Liste der Mitgliedschaftsattribute enthält, die die Gruppen definiert, denen es angehört. • Gruppenobjekt: Eine Liste der Mitgliedschaftsattribute, die alle Objekte auflistet, also entweder Benutzer oder Gruppen, die der Gruppe angehören.
Mitgliedschaftsattribute	Je nachdem, welche Option Sie in der Einstellung Mitgliedschaft definiert in gewählt haben, kann dies entweder der Name des Attributs in einem Mitgliedsobjekt sein, das die Gruppen definiert, dem das Objekt angehört (z. B. <i>memberof</i>) oder der Name des Attributs in einem Gruppenobjekt, mit dem die Objekte aufgelistet werden, die einer Gruppe angehören (z. B. <i>member</i>).

SMTP-Adresseinstellungen

Option	Beschreibung
SMTP-Attribute	Der Name des Attributs eines Verzeichnisbenutzers oder einer Verzeichnisgruppe, das die E-Mail-Adresse des Eintrags enthält Wenn Ihr Verzeichnis mehrere Attributnamen verwendet, um E-Mail-Adressen zu speichern, können Sie eine durch Semikolon (;) getrennte Liste von Attributnamen eingeben. Beispiel: address1@mycompany.com;address2@mycompany.com Anmerkung: Lotus Protector for Mail Security verwendet die Attribute "mail" und "uid".

Einstellungen für SMTP-Domänen

Lotus Protector for Mail Security verwendet eine Liste von SMTP-Domänen für jedes Verzeichnisobjekt während der Nachrichtenverarbeitung und für die Benutzeranmeldung/Benutzerauthentifizierung, um zu ermitteln, ob ein bestimmtes Verzeichnis Informationen zu einer spezifischen Domäne enthält. Die SMTP-Domänenliste fungiert als Filter für Verzeichnissuchfunktionen.

Option	Beschreibung
SMTP-Domänenliste ist leer	Lotus Protector for Mail Security versucht, Informationen aus diesem Verzeichnis für alle Domänenkomponenten abzurufen, die in E-Mail-Adressen gefunden werden.
SMTP-Domänenliste ist nicht leer	Lotus Protector for Mail Security durchsucht die Liste nach der Domänenkomponente einer E-Mail-Adresse. • Wenn sich die Domänenkomponente in der Liste befindet, versucht Lotus Protector for Mail Security Informationen über den Benutzer oder die Gruppe aus diesem Verzeichnis zu beziehen. • Wenn sich die Domänenkomponente nicht in der Liste befindet, wird dieses Verzeichnis nicht nach Informationen über den Benutzer oder die Gruppe abgefragt.

Zeitplanobjekte

Zeitplanobjekte lösen für Lotus Protector for Mail Security bestimmte Tasks zu einem vorgegebenen Zeitpunkt aus, z. B. das Sichern von Protokolldateien und die Erstellung von Quarantäneberichten.

Vorgehensweise

1. Klicken Sie im Navigationsfenster auf **Mail Security > Richtlinienobjekte**.
2. Klicken Sie auf die Registerkarte **Zeitpläne** und anschließend auf **Hinzufügen**.
3. Stellen Sie folgende Informationen bereit:

Option	Bezeichnung
Name	Gibt den Namen des Zeitplanobjekts an.
Zeit	Gibt an, wann Tasks ausgeführt werden sollen, die für die Verwendung dieses Zeitplanobjekts konfiguriert sind. Anmerkung: Das Datum, das automatisch für ein neues Zeitplanobjekt eingegeben wird, entspricht der Zeit des Systems, auf dem Lotus Protector Manager ausgeführt wird, und nicht der aktuellen Systemzeit von Lotus Protector for Mail Security. Die Startzeit kann aber auch der Zeitzone Ihres Web-Browsers oder der Greenwich Mean Time (GMT, Westeuropäische Zeit) entsprechen.
Wiederholen alle	Legt die Zeitspanne zwischen jeder Taskwiederholung fest, die von diesem Zeitplanobjekt ausgelöst werden.

4. Klicken Sie auf **OK**.

Anmerkung: Wenn Sie eine Task planen, verwenden Sie einen absoluten Wert, um den Zeitpunkt der Ausführung festzulegen (beispielsweise planen Sie die Ausführung einer Task für den 2011-10-10 um 10:10). Wenn die Zeit auf dem Lotus Protector for Mail Security-System geändert wird, kann dies Auswirkungen auf den Zeitpunkt haben, zu dem eine geplante Task ausgeführt wird. Weitere Informationen zu diesem Thema finden Sie unter den Einstellungen für Datum und Uhrzeit.

FTP-Server

Auf FTP-Servern werden Protokolldateien gespeichert, die Sie sichern müssen.

Vorgehensweise

1. Klicken Sie im Navigationsfenster auf **Mail Security > Richtlinienobjekte**.
2. Klicken Sie auf die Registerkarte **FTP-Server** und anschließend auf **Hinzufügen**.
3. Geben Sie einen Namen für die Datei an und klicken Sie anschließend auf **Erstellen**.
4. Stellen Sie folgende Informationen bereit:

Option	Bezeichnung
Name	Gibt den Namen des FTP-Serverobjekts an, wie er in Lotus Protector Manager angezeigt werden soll.
Host	Gibt den Hostnamen oder die IP-Adresse des FTP-Servers an, auf dem die Protokolldateien gesichert werden sollen.
Port	Gibt den Port an, an dem die FTP-Server Verbindungen von FTP-Clients akzeptieren.
Stammverzeichnis	Gibt das Basisverzeichnis für dieses FTP-Serverobjekt an. Nachdem Sie sich angemeldet haben, wechselt der FTP-Client gemäß der Konfiguration durch das Objekt zum angegebenen Verzeichnis. Sie können mehrere FTP-Serverobjekte mit dem gleichen FTP-Server für unterschiedliche Basisverzeichnisse konfigurieren. Wenn Sie keine Angabe in diesem Feld machen, wird das Stammverzeichnis des FTP-Servers vom Objekt verwendet.
Benutzer	Gibt den Namen des Benutzers an, der berechtigt ist, sich beim FTP-Server anzumelden.
Kennwort	Gibt das Kennwort des Benutzers an, der im Feld "Benutzer" definiert wurde.

5. Kennwort bestätigen
6. Klicken Sie auf **OK** und anschließend auf **Änderungen speichern**.

Nachrichtenspeicher

Nachrichtenspeicher enthalten die E-Mail-Nachrichten, die Sie archivieren oder unter Quarantäne stellen möchten.

Informationen zu diesem Vorgang

Lotus Protector for Mail Security bietet zwei Typen von Nachrichtenspeichern an, die Sie zum Speichern von E-Mail-Nachrichten verwenden können:

Tabelle 23. Typen von Nachrichtenspeichern

Geschäft	Speichertyp
Nachrichtenspeicher	Speichert blockierte oder verzögerte E-Mail-Nachrichten, einschließlich E-Mail-Nachrichten, die als fehlerhaft oder problematisch eingestuft werden Sie können so viele Nachrichtenspeicher erstellen, wie sie benötigen.
Quarantäne-speicher	Speichert E-Mail-Nachrichten, die bestimmte Kriterien erfüllen, die durch den Administrator definiert werden, wie E-Mail-Nachrichten, die mit Viren infiziert sind oder die vertrauliche Daten enthalten

Achtung: Wenn Sie einen bestehenden Speichertyp von "Nachricht" in "Quarantäne" ändern (oder umgekehrt), wird der vorhandene Speichertyp von Lotus Protector for Mail Security gelöscht und ein neuer Speichertyp wird erstellt. Dabei kann es zu Datenverlusten kommen und die Anzahl der Nachrichten wird möglicherweise nicht ordnungsgemäß ermittelt. Der von Ihnen gelöschte Speichertyp wird möglicherweise im E-Mail-Browser angezeigt, bis er vom System entfernt wird.

Vorgehensweise

1. Klicken Sie im Navigationsfenster auf **Mail Security > Richtlinienobjekte**.
2. Klicken Sie auf die Registerkarte **E-Mail-Speicher**.
3. Wählen Sie eine Option aus:

Wenn Sie folgende Aktion ausführen möchten...	Dann...
Einen neuen Nachrichtenspeicher erstellen	1. Klicken Sie auf Hinzufügen. 2. Wählen Sie aus der Liste Speichertyp den Typ des Nachrichtenrepositorys aus. 3. Geben Sie einen Namen für das Nachrichtenrepository ein. 4. Klicken Sie auf die Registerkarte Allgemein. 5. Legen Sie die Anzahl der Tage fest, die eine E-Mail-Nachricht im Nachrichtenrepository gespeichert werden soll. 6. Wählen Sie aus, wann und wie die E-Mail-Nachricht an den vorgesehenen Empfänger versendet werden soll. 7. Wählen Sie einen Zeitplan aus, um zu definieren, wann Quarantäneberichte an den vorgesehenen Empfänger gesendet werden sollen. 8. Klicken Sie auf die Registerkarte Metadaten. 9. Verwenden Sie Makros, die Teile der E-Mail-Nachricht repräsentieren, die Sie dem Empfänger des Quarantäneberichts senden möchten.

Wenn Sie folgende Aktion ausführen möchten...	Dann...
Legen Sie die Anzahl der Tage fest, die E-Mail-Nachrichten in den Nachrichtenspeichern gespeichert werden sollen.	1. Aktivieren Sie das Kontrollkästchen Aktivieren im Bereich Nachrichtenprotokoll löschen. 2. Legen Sie die Anzahl der Tage fest, die die E-Mail-Nachrichten gespeichert werden sollen. Tipp: Es wird empfohlen, die Nachrichten für sieben Tage zu speichern, um den Verwaltungsaufwand für die Protokolle in der Datenbank im Rahmen zu halten.

In einem Nachrichtenspeicher nach Nachrichten suchen

Dieser Abschnitt beschreibt, wie Sie mithilfe der Seite **E-Mail-Browser (Mail Security > E-Mail-Browser)** nach blockierten, verzögerten oder unter Quarantäne gestellten E-Mail-Nachrichten suchen können, die in einem Nachrichtenspeicher gespeichert sind.

Geben Sie an, ob Sie nach E-Mail-Nachrichten in einem Ordner suchen möchten, ob Sie nach bestimmten E-Mail-Nachrichten in einem Nachrichtenspeicher suchen möchten oder ob Sie Abfragen nach E-Mail-Nachrichten in den Nachrichtenspeichern ausführen möchten.

Ordner

Option	Beschreibung
Quarantänebericht auslösen	Erstellt einen täglichen Quarantänebericht über E-Mail-Nachrichten unter Quarantäne
Löschen	Entfernt eine E-Mail-Nachricht aus dem Nachrichtenspeicher
An spam@kassel.ibm.com senden	Sendet die E-Mail-Nachricht an die Empfänger-E-Mail-Adresse für Spammessages
An notspam@kassel.ibm.com senden	Sendet die E-Mail-Nachricht an die Empfänger-E-Mail-Adresse für Nachrichten, die kein Spam sind
Zustellen	Ermöglicht es Ihnen, die unter Quarantäne gestellten E-Mail-Nachrichten, mit denen Sie arbeiten möchten, zu markieren und stellt die blockierten E-Mail-Nachrichten anschließend an Ihre persönliche E-Mail-Adresse zu
Kopieren	Kopiert eine E-Mail-Nachricht aus einem Nachrichtenspeicher in einen anderen Nachrichtenspeicher
Verschieben	Verschiebt eine E-Mail-Nachricht aus einem Nachrichtenspeicher in einen anderen Nachrichtenspeicher

E-Mails

Option	Beschreibung
Nachrichten-ID	Gibt die Nachrichten-ID an. Sie können anhand der Nachrichten-ID auch nach nicht gespeicherten E-Mail-Nachrichten suchen, wenn Sie in der E-Mail-Sicherheitsrichtlinie die Verfolgung von Nachrichten aktiviert haben (Mail Security > Richtlinie > Nachrichtenverfolgung/Berichterstellung).
Absender	Gibt den Absender der E-Mail-Nachricht an
Empfänger	Gibt den Empfänger der E-Mail-Nachricht an
Betreff	Gibt den Betreff der E-Mail-Nachricht an

Option	Beschreibung
Metadaten	Zeigt Informationen zum Absender, zum Empfänger/zu den Empfängern, zum Erstellungsdatum und zu Anhängen an. Anmerkung: Die Art der Metadaten hängt davon ab, wie Sie Ihr Metadatenfeld für den entsprechenden Nachrichten- oder Quarantänespeicher konfiguriert haben.
Größe	Gibt die Größe der E-Mail-Nachricht an
Ordner	Zeigt die Position der E-Mail-Nachricht im Nachrichtenspeicher an
Im Zeitraum	Legt den Zeitraum fest, in dem nach der E-Mail-Nachricht gesucht werden soll. Verwenden Sie das Format jjjj-mm-tt hh:mm:ss: 2011-12-31 12:45:10.

Anmerkung: Wenn Sie E-Mail-Nachrichten aus einem Nachrichtenspeicher in einen anderen Nachrichtenspeicher kopieren oder verschieben, können Sie keine Metadaten der E-Mail-Nachrichten in dem Nachrichtenspeicher anzeigen, in den Sie die Nachrichten kopiert oder verschoben haben.

Quarantänebericht inaktivieren

In diesem Thema wird erläutert, wie Sie einen Quarantänebericht für einen angegebenen Benutzer inaktivieren. Quarantäneberichte werden standardmäßig aktiviert, um eine E-Mail an Benutzer zu senden, die darüber informiert werden, dass ihre E-Mail aus verschiedenen Gründen unter Quarantäne gestellt wurde.

Vorgehensweise

1. Klicken Sie im Navigationsfenster auf **Mail Security > Richtlinienobjekte**.
2. Klicken Sie auf die Registerkarte **E-Mail-Speicher**.
3. Wählen Sie den Quarantänespeicher und doppelklicken Sie auf das Symbol **Bearbeiten**.
4. Inaktivieren Sie über die Registerkarte **Allgemein** das Kontrollkästchen **Aktivieren**.
5. Klicken Sie auf **OK** und speichern Sie dann Ihre Änderungen.

Schablone für Quarantänebericht

In diesem Abschnitt erhalten Sie Informationen über die Schablonen, die Sie als Basis für den Quarantänebericht verwenden können.

E-Mail-Schablone

Die E-Mail-Schablone muss mindestens das Makro \$(DAILYLIST) enthalten, das durch eine Liste blockierter E-Mail-Nachrichten ersetzt wird. Die Textdatei für Zeilenschablonen definiert dabei jede Zeile dieser Liste.

In der E-Mail-Schablone steht nur eine begrenzte Anzahl von Makros zur Verfügung, die nicht einer aktuellen E-Mail-Nachricht zugeordnet sind, z. B. \$(RECIPIENTNAME). Wenn Lotus Protector for Mail Security Informationen über den Domänennamen oder den LDAP-Benutzernamen enthält, wird dieser durch den entsprechenden Benutzernamen ersetzt. Andernfalls zeigt Lotus Protector for Mail Security die E-Mail-Adresse des Benutzers an.

Wichtig: Verwenden Sie keine Sonderzeichen wie Umlaute bei der Definition der Ordernamen.

Folgende Makros können für die E-Mail-Schablone verwendet werden:

Option	Beschreibung
\$(TAB)	Das Makro "Tabulator" oder \t.
\$(CR)	Das Makro "Neue Zeile" oder \n.
\$(DATE)	Das aktuelle Datum.
\$(DATE.DAY)	Der aktuelle Tag.
\$(DATE.MONTH)	Der aktuelle Monat.
\$(DATE.YEAR)	Das aktuelle Jahr.
\$(DATE.HOUR)	Die aktuelle Stunde.
\$(DATE.MINUTE)	Die aktuelle Minute.
\$(ADMINSERVERPORT)	Der Serverport des Administrators oder Port 4990.
\$(ENDUSERSERVERPORT)	Der Serverport des Endbenutzers oder Port 4991.
\$(MSGSTORE)	Das Stammverzeichnis des Nachrichtenspeichers.
\$(LOGDIR)	Das Protokolldateiverzeichnis.
\$(CONFIGDIR)	Das Konfigurationsverzeichnis.
\$(ENV.<env>)	Der Wert der Umgebungsvariablen <env>.
\$(OPTION.<option>)	Der Wert des Anpassungsparameters <option>.
\$(FILE.<Filename>)	Der Inhalt der Datei <filename>.
\$(ENCODEHTML)	Codiert die HTML-Tags im Makrotext.
\$(NEWMSGSENDER)	Der Wert der Einstellung Neue E-Mail senden als , festgelegt in SMTP > Konfiguration > Global
\$(POSTMASTER)	Sendet die erkannte E-Mail-Nachricht an den ursprünglichen Absender als postmaster@mycompany.com zurück und informiert den Absender, dass die ursprüngliche E-Mail-Nachricht unter Quarantäne gestellt wurde
\$(DAILYLIST)	Dieses Makro wird durch eine Liste blockierter E-Mail-Nachrichten ersetzt.
\$(RECIPIENTNAME)	Die SMTP-Adresse oder der Verzeichnisbenutzername des Empfängers (falls verfügbar).

Option	Beschreibung
\$(RECIPIENT)	Die SMTP-Adresse des Empfängers.
\$(ENDUSERLINK)	Der Wert des Konfigurationselements der Endbenutzerschnittstelle.

Zeilenschablone

Die Zeichenschablone definiert die Ansicht der blockierten E-Mail-Nachrichten und der relevanten Informationen einschließlich des Links, der die Zustellung ermöglicht. Sie können der Schablone angepasste E-Mail-Nachrichten oder Benachrichtigungen hinzufügen, um Informationen bereitzustellen, die von E-Mail-Benutzern benötigt werden.

Der folgende Text zeigt ein Beispiel für eine Zeilenschablone:

```
<tr>
<td width="20%">$(ENCODEHTML $(MSG.FROM))</td>
    $(ENCODEHTML $(MSG.urn:schemas:httpmail:from))</td>
<td width="60%">
    $(ENCODEHTML $(ORIGMSG.SUBJECT))</td>
<td width="20%">
<a href="http://$(HTTPADDRESS):4990/$(CMD.HTTP_DELIVER)">
    Deliver</a><br>
a href="mailto:$(SMTPADDRESS)?subject=$(CMD.DELIVER)">
    Deliver by email</a></td>
</tr>
```

Das vorangehende Beispiel ist eine Kombination aus HTML-Code und Schablonenmakros. Dieses Beispiel zeigt eine Tabellenzeile an und enthält Informationen wie Sender, ursprüngliche Nachrichtenbetreffzeile und die entsprechenden Zustellungslinks. Sie können die Formatierung und die Verwendung der Makros anpassen. Sie können auch eine Test-E-Mail-Nachricht erstellen, um die Regel auszulösen und somit die Ausgabe des Quarantäneberichts zu testen.

Empfänger eines Quarantäneberichts definieren

In diesem Abschnitt wird angegeben, welche E-Mail-Adressen im Nachrichtenspeicher für E-Mail-Nachrichten unter Quarantäne (Quarantänespeicher) im Quarantänebericht enthalten sein sollen.

Informationen zu diesem Vorgang

Eine Empfänger-E-Mail-Adresse wird dem Quarantänespeicher in folgenden Fällen automatisch hinzugefügt:

- Die Domänenkomponente der SMTP-Adresse ist in einer der lokalen SMTP-Domänen angegeben.
- Die Domänenkomponente der SMTP-Adresse ist in der durch Semikolons getrennten Liste mit zusätzlichen Domänen angegeben, die im Anpassungsparameter `msgstore.quarantine_domains` definiert sind. (Eine durch Semikolons getrennte Liste mit SMTP-Domänen, für die eine Quarantäne zulässig ist, zusätzlich zu den lokalen SMTP-Domänen, für die eine Quarantäne zulässig ist.)

Vorgehensweise

1. Klicken Sie im Navigationsfenster auf **Mail Security > Richtlinienobjekte**.
2. Klicken Sie auf die Registerkarte **Vorlagen für Quarantäneberichte** und anschließend auf **Hinzufügen**.
3. Geben Sie einen Namen für den Bericht ein.
4. Klicken Sie auf die Registerkarte **E-Mail-Vorlage**.

Verweis: Informationen zu dieser Vorlage und den von ihr verwendeten Makros finden Sie unter „Schablone für Quarantänebericht“ auf Seite 67.

5. Geben Sie das Makro ein, das Sie für die Vorlage verwenden möchten.
6. Klicken Sie auf die Registerkarte **Zeilenschablone**.

Verweis: Informationen zu dieser Schablone und den von ihr verwendeten Makros finden Sie unter „Schablone für Quarantänebericht“ auf Seite 67.

7. Geben Sie die Makros ein, die Sie für jede Zeile verwenden möchten.
8. Klicken Sie auf **OK** und anschließend auf **Änderungen speichern**.

Inhalte der Dateien überprüfen, die eingehenden E-Mail-Nachrichten angehängt sind

In diesem Thema wird erläutert, auf welche Weise Sie Lotus Protector for Mail Security aktivieren, um Inhalte (Schlüsselwörter, reguläre Ausdrücke, URLs) von Dateien zu untersuchen, die eingehenden E-Mail-Nachrichten angehängt sind.

Informationen zu diesem Vorgang

Die folgenden Dateitypen werden durch Lotus Protector for Mail Security untersucht:

- Microsoft-Dokumente einschließlich Excel, PowerPoint, Word 95, Word 2003, Word 2007, XML
- Oracle Open Office-Dokumente
- Oracle StarOffice-Dokumente
- Lotus 1-2-3-Arbeitsbuchdateien
- PDF-Dateien
- RTF-Dateien
- Einfache Textdateien einschließlich TXT-, HTML-, XML- und andere Dateien
- Archivdateien einschließlich 7Z, BZ2, GZ, TAR, RAR, ZIP

Lotus Protector for Mail Security überprüft den Inhalt der Dateien, die eingehenden E-Mail-Nachrichten angehängt sind, durch Anwendung von Analysemodulen, die in der aktuellen Richtlinienregel aktiviert sind. Gibt die Richtlinienregel zum Beispiel die Verwendung des Schlüsselwort- oder URL-Überprüfungsmoduls an, verwendet Lotus Protector for Mail Security diese Methoden, um die Inhalte aus der angehängten Datei zu überprüfen bevor die E-Mail-Nachricht durch das System geleitet wird. Nachdem der Dateianhang überprüft und als sicher eingestuft wurde (durch Übereinstimmung mit der Richtlinienregel) und die E-Mail-Nachricht mit der Richtlinienregel übereinstimmt, fährt das Richtliniensystem gemäß der definierten Antworten oder Aktionen (Zulassen, Blockieren, Fortfahren) mit der Verarbeitung der E-Mail-Nachricht fort.

Vorgehensweise

1. Klicken Sie im Navigationsfenster auf **Mail Security > Richtlinie**.
2. Klicken Sie auf die Registerkarte **Analyse des Dateianhangs**.
3. Aktivieren Sie das Kontrollkästchen **Analyse des Dateianhangs aktivieren**.

Wichtig: Die Aktivierung dieser Funktion kann eine Reduzierung des durchschnittlichen Durchsatzes von E-Mail-Nachrichten nach sich ziehen, da Lotus Protector for Mail Security umfangreiche Datenmengen untersucht.

DNSBL-/Spamdatenflusseinstellungen konfigurieren

In diesem Abschnitt wird erläutert, wie die Spamdatenflussteuerung konfiguriert und wie die Liste der DNSBL-Server (Domain Name Server Block List) verwaltet wird, die von Lotus Protector for Mail Security verwendet werden.

Einstellungen für den Spamdatenfluss

Das Modul für Spamdatenflussteuerung verwendet verschiedene Kriterien für die Ähnlichkeit von E-Mails. Anhand dieser Kriterien für die Ähnlichkeit wird für jede E-Mail-Nachricht eine eindeutige Signatur erstellt. Jeder Signatur ist eine Liste eindeutiger Domänen zugeordnet, die von der SMTP-Adresse des Senders extrahiert werden (z. B. mycompany.com von joe@mycompany.com) sowie eine Trefferzahl für das Vorkommen in einem bestimmten Zeitrahmen. Wenn die Domänenliste für eine Signatur eine vordefinierte Anzahl von Einträgen enthält, wird die Trefferzahl für diese Signatur von dem Analysemodul für Spamdatenflussteuerung jedes Mal erhöht, sobald diese Signatur in einer E-Mail-Nachricht gefunden wird.

Sollte innerhalb eines bestimmten Zeitrahmens der Signaturzähler einen vordefinierten Schwellenwert überschreiten, wird jede nachfolgende, vom Modul für Spamdurchflussteuerung analysierte E-Mail-Nachricht abgeglichen.

Tabelle 24. Einstellungen für den Spamdatenfluss

Option	Beschreibung
Analysefenster	Gibt die Anzahl der Sekunden an, die das Analysemodul für die Aufbewahrung und Verwaltung einer bestimmten Signatur aufwendet. Diese Einstellung wirkt sich auch auf die Zeitspanne aus, die das Analysemodul für den Abgleich einer bestimmten Signatur aufwendet.
Mindesttreffer	Gibt die erforderliche Anzahl von Vorkommen in dem Fluss der analysierten E-Mail-Nachrichten für eine bestimmte Signatur an, bevor weitere nachfolgende Vorkommen der Signatur als Übereinstimmung gewertet werden.

DNSBL-Listen

Ein DNSBL-Server enthält eine Liste von IP-Adressen für Hosts, die für das Senden oder Weiterleiten von unerwünschten E-Mail-Nachrichten bekannt sind. Die Qualität einer DNSBL-Liste beruht auf den angewandten Methoden der DNSBL-Server, mit denen die Liste von bekannten Spammern erstellt wird.

Tabelle 25. DNSBL-Listeneinstellungen

Option	Beschreibung
Schwellenwert	Wenn die Summe aller DNSBL-Serverübereinstimmungsquoten diesen Wert übersteigt, wird die analysierte E-Mail-Nachricht für das Spam-DNSBL-Analysemodul als Übereinstimmung gewertet.
Spam-DNSBL-Server	Der Hostname des DNSBL-Servers, den Sie verwenden möchten (z. B. dnsbl.cobion.com).
Übereinstimmungsquote	Gibt den Wert an, der zu der Gesamtquote hinzuaddiert wird, wenn dieser bestimmte DNSBL-Server ein positives Ergebnis zurückgibt. Dieser Wert kann zur Feinabstimmung des Mechanismus verwendet werden, wenn Sie DNSBL-Server mit unterschiedlichen Zuverlässigkeiten verwenden.

Anmerkung: Wenn DNSBL-Suchvorgänge als DNS-Anforderungen ausgeführt werden, kann der DNSBL-Abgleich schnell durchgeführt werden. Da die DNS-Anforderungen auf Anfrage des Netzes verwendet werden, verzögert sich jedoch möglicherweise die Analyse der E-Mail-Nachricht solange, bis Lotus Protector for Mail Security eine Antwort von verfügbaren DNSBL-Servern erhält. Die Verwendung einer großen Anzahl von DNSBL-Servern kann die Leistung von Lotus Protector for Mail Security beeinträchtigen.

Zugriffsberechtigungen für die Endbenutzerschnittstelle einrichten

In diesem Abschnitt wird erläutert, wie Sie die Zugriffsberechtigungen für die Endbenutzerschnittstelle einrichten, damit Benutzer unter Quarantäne gestellte E-Mail-Nachrichten suchen und anzeigen, persönliche Blockierlisten und persönliche Zulassungslisten verwalten und ihre täglichen Quarantäneberichte generieren und zustellen können.

Sie können entweder die volle Berechtigung für die Endbenutzerschnittstelle erteilen, indem Sie die Option **Standardzugriffsmodus** auf *Gewährt* festlegen, oder eine differenziertere Konfiguration durch Hinzufügen von Who-Objekten zur Liste erstellen. Der Standardzugriffsmodus wird für alle Benutzer angewendet, die nicht durch Who-Objekte in der Liste dargestellt werden.

Achtung: Wenn Sie die Endbenutzerschnittstelle verwenden möchten, muss der Zugriff auf die Endbenutzerschnittstelle in der Firewall von Lotus Protector for Mail Security auf der Firewallseite entsprechend ermöglicht werden.

Tabelle 26. Einstellungen für Endbenutzerschnittstelle

Option	Beschreibung
Standardzugriffsmodus	Gibt den Zugriffsmodus für Benutzer an, die von keinem Who-Objekt auf der Zugriffsliste repräsentiert werden: • Gewährt: Benutzer, die von keinem der Who-Objekte repräsentiert werden, haben eine Zugriffsberechtigung auf die Endbenutzerschnittstelle. • Verweigert: Der Zugriff wird den Benutzern verweigert, die von keinem der Who-Objekte auf der Liste repräsentiert werden.
URL für Endbenutzerschnittstelle	Stellt die URL-Adresse einer Website bereit, auf die Benutzer zugreifen können, um die Endbenutzerschnittstelle zu verwenden. Diese URL wird auch in den Quarantäneberichten verwendet.
Who	Gibt an, dass ein bestimmter Benutzer oder eine bestimmte Gruppe, repräsentiert durch ein Who-Objekt, über einen speziellen Zugriffsmodus verfügt.
Zugriffstyp	Gibt den Zugriffstyp für ein bestimmtes Who-Objekt an: • Gewährt: Benutzer, die durch das Who-Objekt repräsentiert werden, haben Zugriff auf die Endbenutzerschnittstelle. • Verweigert: Der Zugriff wird den Benutzern verweigert, die durch das Who-Objekt repräsentiert werden.

E-Mail-Nachrichten verfolgen

Dieser Abschnitt beschreibt, wie E-Mail-Nachrichten, die Lotus Protector for Mail Security passieren, bis zu ihrer Zustellung oder Löschung verfolgt werden können.

Nachrichtenverfolgung

Option	Beschreibung
Verfolgungsstufe	Legt fest, welche Stufe Lotus Protector for Mail Security für die Verfolgung des Datenflusses der E-Mail-Nachrichten im System verwenden soll: • Deaktiviert: Lotus Protector for Mail Security verfolgt keine E-Mail-Nachrichten. • Standard: Lotus Protector for Mail Security verfolgt folgende Informationen einer E-Mail-Nachricht: – Zeitpunkt des Eingangs der E-Mail-Nachricht auf SMTP-Ebene im System – Zeitpunkt der Verarbeitung der E-Mail-Nachricht durch die E-Mail-Sicherheitsrichtlinie – Zeitpunkt der Zustellung der E-Mail-Nachricht auf SMTP-Ebene Diese Option ist nützlich, wenn Sie die Empfängerüberprüfung auf SMTP-Ebene verwenden, um folgende Informationen einer E-Mail-Nachricht zu verfolgen: – Zeitpunkt und Grund der Zurückweisung oder Löschung der E-Mail-Nachricht auf SMTP-Ebene – Verarbeitungsablauf der E-Mail-Nachricht im System (z. B. welcher sendende Server die E-Mail-Nachricht angenommen hat) – Verzögerung zwischen der Annahme der E-Mail-Nachricht auf SMTP-Ebene und der Analyse der Nachricht – SMTP-Server, der die E-Mail-Nachricht zugestellt hat • Ausführlich (weitere Einzelheiten): Lotus Protector for Mail Security verwendet die Informationen, die aus folgenden Quellen zusammengestellt wurden: – Standardmodus (siehe oben) – Protokollinformationen – Analysedetails Diese Option ist nützlich, wenn Sie sich an IBM Support wenden müssen hinsichtlich eines Problems, das in Zusammenhang mit E-Mail-Nachrichten auftritt, die über Lotus Protector for Mail Security weitergeleitet werden.

Kapitel 4. Benachrichtigungen, Systemereignisse und Protokolle

In diesem Kapitel wird beschrieben, wie Benachrichtigungen konfiguriert werden, die Sie oder andere benachrichtigen, sobald ein bestimmtes Ereignis stattfindet. Des Weiteren wird beschrieben, wie Systemereignisse angezeigt und verwaltet und Protokolldateien angezeigt und erstellt werden.

E-Mail-Benachrichtigungen und SNMP-Statusmeldungen verwenden

In diesem Abschnitt wird erläutert, wie Statusmeldungen eingerichtet werden, die Sie über Systemereignisse benachrichtigen.

Vorgehensweise

1. Klicken Sie im Navigationsfenster auf **System > E-Mail- und SNMP-Statusmeldungen**.
2. Klicken Sie auf die Registerkarte **Statusmeldungen-Konfiguration**.
3. Aktivieren Sie eines der folgenden Kontrollkästchen für die Statusmeldungen-Protokollierung:

Option	Bezeichnung
Statusmeldungen bei Mail Security-Ereignissen senden	Benachrichtigt Sie, wenn ein E-Mail-Sicherheitsereignis aufgetreten ist.
Statusmeldungen bei Systemfehlerereignissen senden	Benachrichtigt Sie, wenn ein Systemfehler aufgetreten ist. Sie erhalten eine Fehlerbeschreibung und eventuell weitere Informationen zur Ursache des Fehlers.
Statusmeldungen bei Systemwarnungsereignissen senden	Benachrichtigt Sie, wenn ein Problem in Lotus Protector for Mail Security selbst aufgetreten ist.
Statusmeldungen bei Systeminformationsereignissen senden	Benachrichtigt Sie darüber, welche Aktionen Benutzer in Lotus Protector for Mail Security ausgeführt haben, z. B. Ändern von Kennwörtern, Herunterladen von Protokollen oder Bearbeiten von Parametern. Anmerkung: Wenn Sie die Einstellung Statusmeldungen für Systeminformationsereignisse senden aktivieren und anschließend Lotus Protector for Mail Security neu starten, erhalten Sie möglicherweise folgende Nachricht im Message.log oder als SMTP- oder SNMP-Benachrichtigung: Kritischer Eingangspunkt (ResponsesdkGetObject) für Bibliothek... Dies ist ein erwartetes Verhalten bei Systembenachrichtigungen. Es ist kein Benutzereingriff erforderlich.

Option	Bezeichnung
Zustellungsmethoden für Benachrichtigung	Gibt an, wie Ereignisbenachrichtigung und Nachrichtenübermittlung erfolgen sollen: • An E-Mail-Adresse/E-Mail-Namen senden: Sendet eine Benachrichtigung an die im Standard-E-Mail-Namen angegebene Adresse, wenn die Statusmeldung auftritt • An SNMP-Trap senden: Löst einen SNMP-Trap aus, wenn die Statusmeldung auftritt. • SNMP konfigurieren: – SSH: Gewährleistet die sichere Anmeldung für Windows- und Unix-Clients sowie Server. – SNMP-Get: Fragt SNMP-Informationen zu einem Netzserver ab. - Systemname: Gibt das Ziel der SNMP-Abrufanforderung an. - Systemadresse: Gibt die Adresse des Servers im Netz an. - Kontaktinformation: Gibt den Ansprechpartner für das System anhand des SNMP-Community-Namens an. - Get-Community: Gibt den SNMP-Community-Namen an (öffentlich oder privat), der in der SNMP-Abrufanforderung verwendet wird. SNMP-Trap: - Trapempfängeradresse: Gibt die Server-IP-Adresse an, unter der der SNMP-Manager ausgeführt wird. Lotus Protector for Mail Security muss auf den SNMP-Host zugreifen können, um E-Mail-Benachrichtigungen senden zu können. - Trap-Community: Gibt den entsprechenden Community-Namen an (öffentlich oder privat). - Trap-Version: • V1: Simple Network Management Protocol Version 1 • V2c: Community-Based Simple Network Management Protocol Version 2

4. Klicken Sie auf **Änderungen speichern**.

Empfänger von Statusmeldungen definieren

In diesem Abschnitt wird erläutert, wie Sie Statusmeldungen an eine angegebene E-Mail-Adresse oder an eine E-Mail-Gruppe senden können.

Vorgehensweise

1. Klicken Sie im Navigationsfenster auf **System > E-Mail- und SNMP-Statusmeldungen**.
2. Klicken Sie auf die Registerkarte **Statusmeldungen-Konfiguration**.
3. Klicken Sie im Abschnitt **E-Mail-Konfiguration** auf **Hinzufügen**.
4. Geben Sie folgende Informationen ein:

Option	Bezeichnung
Name	Gibt die Konfiguration der E-Mail-Statusmeldungen an.
SMTP-Host	Gibt den Mail-Server an (als vollständig qualifizierten Domännennamen oder IP-Adresse).
An	Gibt die E-Mail-Adresse des beabsichtigten Empfängers an (Einzelperson oder Gruppe).
Betreffformat	Ermöglicht die Eingabe von Text und die Auswahl aus einer Liste von Nachrichtenbetrefffeldern. Sie können mehrere Felder einfügen.
Textformat	Ermöglicht die Eingabe von Text und die Auswahl aus einer Liste von Textbetrefffeldern. Sie können mehrere Felder einfügen.

Erweiterte Parameter für die Ereignisbenachrichtigung konfigurieren

In diesem Abschnitt wird erläutert, wie Sie erweiterte Parameter verwenden, um das Verhalten von Lotus Protector for Mail Security bei der Ereignisbenachrichtigung genauer festlegen zu können.

Vorgehensweise

1. Klicken Sie im Navigationsfenster auf **System > E-Mail- und SNMP-Statusmeldungen**.
2. Klicken Sie auf die Registerkarte **Erweiterte Einstellungen**.
3. Wird der Parameter, den Sie bearbeiten möchten, in der Registerkarte **Erweiterte Einstellungen** nicht angezeigt, führen Sie die folgenden Schritte aus:
 - a. Klicken Sie auf das Symbol **Hinzufügen**.
 - b. Geben Sie den Namen des Parameters ein.
 - c. Geben Sie eine Beschreibung des Parameters ein.
 - d. Geben Sie den Werttyp und den Wert des Parameters ein.
4. Klicken Sie auf das Wert- oder auf das Beschreibungsfeld und ändern Sie die Einstellung, wenn der Parameter, den Sie optimieren möchten, bereits auf der Registerkarte **Erweiterte Einstellungen** angezeigt wird.

Achtung: In den meisten Fällen müssen Sie die erweiterten Parameter nicht ändern. Ändern Sie diese Parameter nur, wenn Sie vom technischen Support von IBM dazu aufgefordert werden.

Parametername	Beschreibung	Standardwert
Trace.csf.filename	Gibt den Namen der CSF-Tracedatei an.	/var/spool/crm/CrmTrace.txt
Trace.csf.level	Gibt die Tracestufe für die Informationen an, die in der CSF-Tracedatei angezeigt werden sollen. Die Einstellungen für die Tracestufe sind folgende: • 0 = Keine Verfolgung • 1 = Nur Fehler • 2 = Nur Fehler und Warnungen • 3 = Nur Fehler, Warnungen und wichtige Hinweise • 4 = Nur Fehler, Warnungen, wichtige Hinweise und Informationsnachrichten • 5 = Fehler, Warnungen, wichtige Hinweise, Informationsnachrichten und Debugnachrichten • 6 = Alle Stufen von 1 bis 5	0
Trace.other.filename	Gibt die DFV-Tracedatei an.	/var/spool/crm/CrmCommTrace.txt
Trace.other.level	Gibt die Tracestufe für die Informationen an, die in der DFV-Tracedatei angezeigt werden sollen. Die Einstellungen für die Tracestufe sind folgende: • 0 = Keine Verfolgung • 1 = Nur Fehler • 2 = Nur Fehler und Warnungen • 3 = Nur Fehler, Warnungen und wichtige Hinweise • 4 = Nur Fehler, Warnungen, wichtige Hinweise und Informationsnachrichten • 5 = Fehler, Warnungen, wichtige Hinweise, Informationsnachrichten und Debugnachrichten • 6 = Alle Stufen von 1 bis 5	0

5. Klicken Sie auf **OK**.

Systembezogene Ereignisse verwalten

In diesem Abschnitt wird erläutert, wie Sie E-Mail-Sicherheitsereignisse, Systemnachrichten sowie Updateprobleme anzeigen und verwalten, die vom System in einem angegebenen Zeitraum generiert werden.

Vorgehensweise

1. Klicken Sie im Navigationsfenster auf **System > Ereignisse**.
2. Wählen Sie im Feld **Filter** die Option **Ein** aus.
3. Geben Sie folgende Informationen ein:

Option	Bezeichnung
Startdatum	Weist den Filter an, zu diesem Termin mit der Filterung zu beginnen. Dabei wird folgendes Format verwendet: jjjj-mm-tt hh:mm:ss (z. B. 2011-12-31 12:45:10)
Enddatum	Weist den Filter an, die Filterung zu diesem Termin zu beenden. Dabei wird folgendes Format verwendet: jjjj-mm-tt hh:mm:ss (z. B. 2011-12-31 12:45:10)
Wertigkeit	Gibt die Sicherheitsstufe des Ereignisses an: • Hoch: Sicherheitsprobleme, die einen sofortigen Fernzugriff, lokalen Zugriff oder die sofortige Ausführung von Code oder Befehlen ohne autorisierte Berechtigung ermöglichen. Beispiel: Die meisten Fälle von Pufferüberläufen, Backdoors, Standardkennwörtern oder fehlenden Kennwörtern sowie Umgehungen der Sicherheitsfunktionen von Firewalls und anderen Netzkomponenten. • Mittel: Sicherheitsprobleme, die möglicherweise unbefugte Zugriffe oder die Ausführung von Code ermöglichen, indem komplexe und langwierige Nutzungsvorgänge oder Vorgänge mit niedrigem Sicherheitsrisiko auf wichtigen Internetkomponenten ausgeführt werden. Beispiel: Cross-Site Scripting, Man-in-the-Middle-Attacken, SQL-Injection, Denial-of-Service-Attacken bei wichtigen Anwendungen und Denial-of-Service-Attacken, bei denen Systeminformationen offen gelegt werden (z. B. Kerndateien). • Niedrig: Sicherheitsprobleme, bei denen der Service verweigert wird oder systemfremde Informationen offen gelegt werden, die für strukturierte Attacken auf ein Ziel verwendet werden können, jedoch nicht, um direkten unbefugten Zugriff zu erlangen. Beispiel: Brute-Force-Attacken, Offenlegung von systemfremden Informationen Konfigurationen, Pfade) und Denial-of-Service-Attacken.
Ereignistyp	Gibt den Ereignistyp an, den Sie aus der Liste herausfiltern möchten.
Ereignisname	Gibt einen eindeutigen, beschreibenden Namen für das Ereignis an.

4. Klicken Sie auf **Ergebnisse filtern**.

Protokolldateien anzeigen

Dieser Abschnitt beschreibt die Vorgehensweise beim Anzeigen oder Herunterladen von Protokolldateien, um Ihnen bei der Fehlerbehebung mit Lotus Protector for Mail Security zu helfen.

Vorgehensweise

1. Klicken Sie im Navigationsfenster auf **System > Protokolldateien**.
2. Wählen Sie unter **Verzeichnisse durchsuchen** ein Verzeichnis aus.
3. Wählen Sie die Protokolldatei aus, die Sie anzeigen möchten.
4. Optional: Klicken Sie auf die Schaltfläche **Herunterladen**, um die Protokolldatei in ein Verzeichnis Ihrer Wahl herunterzuladen.

Diagnosedatei generieren

Dieser Abschnitt beschreibt die Vorgehensweise beim Erfassen von Informationen, die der technische Support von IBM verwenden kann, um Sie bei der Fehlerbehebung für Probleme in Lotus Protector for Mail Security zu unterstützen.

Vorgehensweise

1. Klicken Sie im Navigationsfenster auf **Support > Diagnosedatei**.
2. Legen Sie die Anzahl der Tage fest, für die Sie in der Support-Datendatei Informationen erfassen möchten.
3. Klicken Sie auf **Jetzt generieren**.

Anmerkung: Die Support-Datendatei verwendet die Dateinamenerweiterung TGZ.

Protokolldateien zum Ermitteln der Ursache einer blockierten E-Mail-Nachricht anzeigen

Datei	Beschreibung
/var/log/messages	Zeigt an, ob eine E-Mail-Nachricht infolge einer Richtlinienregel blockiert wurde.
/etc/xmail/logs/	Zeigt an, ob eine E-Mail-Nachricht infolge eines SMTP-bezogenen Problems blockiert wurde.

Kapitel 5. Vordefinierte Berichte

In diesem Kapitel wird die Verwendung von vordefinierten Berichten für den Status Ihrer E-Mail-Sicherheit beschrieben.

Vordefinierte Berichte

Lotus Protector for Mail Security umfasst vordefinierte Berichte, die Details zum aktuellen Systemstatus wie Datenfluss, den häufigsten Absendern und internen Empfängern von spambasierten E-Mail-Nachrichten sowie zu der aktuell geltenden Sicherheitsrichtlinie bereitstellen.

Vordefinierte Berichte

Lotus Protector for Mail Security stellt die folgenden vordefinierten Berichte zur Verfügung:

Tabelle 27. Vordefinierte Berichte

Bericht	Beschreibung
Kurzübersicht	Zeigt den Gesamtdurchsatz von Lotus Protector for Mail Security gegenüber den E-Mail-Nachrichten an, die Aktionen erforderten, sowie unter Quarantäne gestellte E-Mail-Nachrichten gegenüber E-Mail-Nachrichten, die aus der Quarantäne freigegeben wurden
Datenverkehrsüberwachung	Stellt Informationen zum Datenaustausch im Netz im angegebenen Zeitraum bereit.
Übereinstimmende Regeln	Stellt Informationen darüber bereit, welche Richtlinienregeln im angegebenen Zeitraum übereinstimmen.
Richtlinienkonfiguration	Stellt Informationen zu der aktuell gültigen E-Mail-Sicherheitsrichtlinie bereit.
Top 10-Responses	Stellt Informationen zu den 10 häufigsten Interventionen bereit, die von der E-Mail-Sicherheitsrichtlinie im angegebenen Zeitraum ausgeführt wurden.
Top 10-Analysemodule	Stellt Informationen zu den 10 häufigsten Analysemodulen bereit, die mit den in der E-Mail-Sicherheitsrichtlinie aktivierten Analysemodulen übereinstimmen.
Top 10-Empfänger	Stellt Informationen zu den 10 häufigsten Empfängern nach der Anzahl der empfangenen E-Mail-Nachrichten bereit
Top 10-Sender	Stellt Informationen zu den 10 häufigsten Absendern nach der Anzahl der gesendeten E-Mail-Nachrichten bereit
Top 10-Viren	Stellt Informationen zu den 10 häufigsten Viren nach der Anzahl der infizierten E-Mail-Nachrichten bereit

Vordefinierten Bericht generieren

Dieser Abschnitt beschreibt die Vorgehensweise bei der Generierung eines vordefinierten Berichts.

Vorbereitende Schritte

Stellen Sie sicher, dass Sie **Berichterstellung aktiviert** in der Registerkarte **Nachrichtenverfolgung/Berichterstellung** auf der Seite **Mail Security-Richtlinie** ausgewählt haben.

Vorgehensweise

1. Klicken Sie im Navigationsfenster auf **Mail Security > Berichterstellung**.
2. Wählen Sie nach Möglichkeit eine Datenquelle, eine Startzeit und eine Endzeit für den Bericht aus.
3. Wählen Sie einen Bericht aus und klicken Sie anschließend auf **Generieren**.

Zeitplanung bei der Ausführung von vordefinierten Berichten

Dieser Abschnitt beschreibt die Vorgehensweise bei der Planung eines vordefinierten Berichts von Lotus Protector for Mail Security für bestimmte Intervalle.

Vorgehensweise

1. Klicken Sie im Navigationsfenster auf **Mail Security > Richtlinie**.
2. Klicken Sie auf die Registerkarte **Nachrichtenverfolgung/Berichterstellung**.
3. Aktivieren Sie das Kontrollkästchen **Berichterstellung aktiviert**.
4. Stellen Sie folgende Informationen bereit:

Option	Bezeichnung
Tage aufzubewahren	Stellt die Anzahl der Tage ein, die der Bericht im Dateisystem aufbewahrt wird.
Allgemeine Berichterstellung	• SNMP-Trap aktiviert: Sendet einen SNMP-Trap an einen SNMP-Server. Diese enthält die IP-Adressen der Ereignisquelle, die angeforderten URLs und die nicht eingehaltenen E-Mail-Kategorien. • Systemprotokoll aktiviert: Schreibt jedes Mal in eine Protokolldatei, wenn ein Bericht ausgeführt wird. • Datenbank aktiviert: Speichert den Bericht in der Lotus Protector for Mail Security-Datenbank.

Option	Bezeichnung
Geplante Berichte konfigurieren	• Cluster: Gibt an, ob Lotus Protector for Mail Security zu einem Cluster gehört. (In den Berichten werden Informationen zu allen Computern im Cluster-Szenario erfasst.) • Bericht: Legen Sie den Bericht fest, der ausgeführt werden soll. • An: Gibt an, an welche E-Mail-Adressen der Bericht gesendet werden soll • Zeitplan: Gibt an, zu welchem Zeitpunkt der Bericht ausgeführt werden soll (wie unter Mail Security > Richtlinienobjekte > Zeitpläne festgelegt). Beispiel: Geben Sie Täglich 7:00 ein, um festzulegen, dass der Bericht täglich um 7 ausgeführt werden soll. • Zeitbereich: Gibt an, ob der Bericht innerhalb eines relativen Zeitbereichs (Zeitspanne im Verhältnis zur aktuellen Zeit) oder zu einem absoluten Zeitpunkt (mit fester Start- und Endzeit) ausgeführt werden soll.

5. Klicken Sie auf **OK** und anschließend auf **Einstellungen ausführen**.

Kapitel 6. Sicherung und Wiederherstellung

In diesem Kapitel wird beschrieben, wie Momentaufnahmedateien mit Konfigurationseinstellungen für Lotus Protector for Mail Security verwaltet und vollständige Systemsicherungen der Lotus Protector for Mail Security-Einstellungen erstellt werden.

Sicherungsarten

Sie können Momentaufnahmedateien von Konfigurationseinstellungen erstellen oder eine vollständige Systemsicherung des Lotus Protector for Mail Security-Betriebssystems und der aktuellen Konfigurationseinstellungen ausführen.

Konfigurationssicherung

Eine Konfigurationssicherung ist eine Momentaufnahmedatei, die sämtliche Lotus Protector for Mail Security-Konfigurationseinstellungen speichert. Sie können über mehrere Momentaufnahmedateien mit den Einstellungen für unterschiedliche Konfigurationen verfügen.

Ebenso haben Sie die Möglichkeit, zusätzliche Momentaufnahmedateien von Einstellungen zu erstellen, wenn Sie z.B. neue Richtlinieneinstellungen für Lotus Protector for Mail Security testen möchten. Die Momentaufnahmedatei `factoryDefault.settings` enthält die ursprünglichen, standardmäßigen Lotus Protector for Mail Security -Einstellungen. Erstellen Sie möglichst immer eine Momentaufnahmedatei, bevor Sie Ihre Konfigurationseinstellungen ändern.

Systemsicherung

Mithilfe einer Systemsicherung wird das vollständige Abbild des Betriebssystems und der aktuellen Konfigurationseinstellungen von Lotus Protector for Mail Security abgespeichert. Sie können nur eine Systemsicherungsdatei anlegen. Wenn Sie mithilfe einer Systemsicherung eine Wiederherstellung durchführen, stellen Sie einen früheren Status von Lotus Protector for Mail Security wieder her.

Konfigurationseinstellungen sichern

Durch das Update von Lotus Protector for Mail Security wird sichergestellt, dass Ihr Produkt stets auf dem neuesten Stand ist. Vor der Installation von Updates, die sich auf die ursprünglichen Konfigurationseinstellungen auswirken können, wird Ihr System gesichert.

Informationen zu diesem Vorgang

Erstellen Sie eine Momentaufnahme der ursprünglichen Konfigurationseinstellungen für Lotus Protector for Mail Security, bevor Sie Firmware-Updates oder Änderungen an den Konfigurationseinstellungen vornehmen. Sie können später zusätzliche Momentaufnahme erstellen, wenn Sie andere Konfigurationseinstellungen verwenden oder neue Richtlinieneinstellungen testen möchten.

Die Datei `factoryDefault.settings` enthält standardmäßig die ursprünglichen Konfigurationseinstellungen von Lotus Protector for Mail Security. Erstellen Sie möglichst immer eine Momentaufnahme, bevor Sie Ihre Konfigurationseinstellungen ändern.

Vorgehensweise

1. Klicken Sie im Navigationsfenster auf **Sicherung und Wiederherstellung > System**.
2. Klicken Sie auf **Konfigurationssicherung verwalten**.
3. Wählen Sie im Abschnitt **Konfigurationssicherungen** eine Option aus:

Option	Bezeichnung
Momentaufnahme erstellen	1. Klicken Sie auf Neu. 2. Geben Sie einen Namen für die Momentaufnahme ein und klicken Sie auf Erstellen.
Momentaufnahme wiederherstellen	Wählen Sie die Momentaufnahme aus, die Sie wiederherstellen möchten, und klicken Sie auf Wiederherstellen .
Momentaufnahme löschen	Wählen Sie die Momentaufnahme aus, die Sie löschen möchten, und klicken Sie auf Löschen .
Momentaufnahme hochladen	1. Klicken Sie auf Neu. 2. Geben Sie den Namen der Momentaufnahme ein, die Sie hochladen möchten, und klicken Sie auf Hochladen.
Momentaufnahme herunterladen	Wählen Sie die Momentaufnahme aus, die Sie herunterladen möchten, und klicken Sie auf Herunterladen .

Vollständige Systemsicherungen erstellen

In diesem Abschnitt wird erläutert, wie Sie ein vollständiges Image des Betriebssystems und der aktuellen Konfigurationseinstellungen von Lotus Protector for Mail Security erstellen, bevor Sie Firmware-Updates oder Momentaufnahmedateien anwenden, die sich auf die ursprünglichen Konfigurationseinstellungen auswirken.

Vorgehensweise

1. Klicken Sie im Navigationsfenster auf **Sicherung und Wiederherstellung > System**.
2. Klicken Sie auf **Systemsicherung verwalten**.
3. Wählen Sie eine Option aus:

Wenn Sie folgende Aktion ausführen möchten...	Dann...
Vollständige Systemsicherung erstellen	Klicken Sie auf Vollständige Systemsicherung erstellen .
Systemsicherung wiederherstellen	Klicken Sie auf Systemsicherung wiederherstellen .

Wichtig: Die IP-Adresse für Lotus Protector for Mail Security ist während der Sicherung nicht verfügbar und Sie können nicht vom Browserfenster auf Lotus Protector Manager zugreifen.

Kapitel 7. Updates

In diesem Kapitel wird beschrieben, wie Sie Updates für Firmware, Datenbanken und Sicherheitskomponenten von Lotus Protector for Mail Security herunterladen und installieren können.

Wichtig: Aktualisieren Sie Lotus Protector for Mail Security so bald wie möglich nach der ErstKonfiguration, um sicherzustellen, dass Ihr Schutz vor Zugriffen auf dem neuesten Stand ist. Mithilfe von Updates wird sichergestellt, dass Lotus Protector for Mail Security stets über die neuesten Updates für Korrekturen, Features, Sicherheitskomponenten und Datenbanken verfügt.

Aktuellen Status und Lizenzen für den Spamschutz anzeigen

In diesem Abschnitt wird erläutert, wo der aktuelle Status der Spamschutzdatenbanken und -lizenzen von Lotus Protector for Mail Security angezeigt werden kann.

Die Updates für E-Mail-Sicherheit stellen tägliche Updates von URLs und Spamsignaturen für Lotus Protector for Mail Security zur Verfügung.

Wichtig: Damit die lokale E-Mail-Sicherheitsdatenbank aktuell bleibt, wird empfohlen, mindestens einmal täglich ein Update durchzuführen.

Tabelle 28. Status von Komponenten und Lizenzen

Option	Beschreibung
Komponenten	Zeigt den aktuellen Status der folgenden Komponenten an: • Mail Security-Datenbank: Die Mail Security-Datenbank umfasst URLs und Klassifizierungen von Webseiten, einschließlich Spamsignaturen aller bekannten Spams (zusammengestellt von Spam-Collectors und weiteren Quellen). • Systempakete: Die Systempakete enthalten die aktuellen Hotfixes und Patches für Kernkomponenten des Systems. • Firmware des Systems: Die Firmwareversion der Software von Lotus Protector for Mail Security. • Antivirensignaturen: Die Antivirensignaturen enthalten eine Liste mit von IBM definierten Virusdefinitionen für bekannte Viren.
Lizenzen	Zeigt den aktuellen Lizenzstatus für die folgenden Module an: • Mail Security-Lizenz: Ermöglicht die Installation von Spamschutzupdates für Lotus Protector for Mail Security. • Antivirus: Ermöglicht die Installation von Antivirenupdates für Lotus Protector for Mail Security.

Aktualisierungsprozess automatisieren

Dieser Abschnitt beschreibt die Vorgehensweise bei der Automatisierung des Prozesses zum Überprüfen, Herunterladen und Installieren der Updates von Lotus Protector for Mail Security.

Informationen zu diesem Vorgang

IBM veröffentlicht regelmäßig Updates für Lotus Protector for Mail Security. Bei diesen Updates kann es sich entweder um Sicherheitskomponentenupdates oder Produktupdates handeln. Sie können festlegen, wie häufig Lotus Protector for Mail Security nach Updates suchen soll. Dabei können Sie gesondert festlegen, wie häufig Lotus Protector for Mail Security nach Sicherheitskomponentenupdates und wie häufig nach Produktupdates gesucht werden soll.

Vorgehensweise

1. Klicken Sie im Navigationsfenster auf **Updates > Automatische Updates**.
2. Klicken Sie auf die Registerkarte **Aktualisierungseinstellungen**.
3. Stellen Sie folgende Informationen bereit:

Option	Bezeichnung
HTTPS-Proxy konfigurieren	Gibt die Proxy-Serverinformationen an, wenn Lotus Protector for Mail Security einen Proxy-Server für den Zugriff auf den Aktualisierungsserver verwendet: • Adresse: Gibt die Adresse des Proxy-Servers an. Anmerkung: Die folgenden Authentifizierungsausnahmen müssen hinzugefügt werden, wenn kein statischer Proxybenutzer verfügbar ist: – *.ibm.com – license.cobion.com – IP-Adressen, die aufgelöst werden in filterdb.ibm.com (derzeit 85.25.143.136, 85.25.252.124, 87.106.3.48, 87.106.21.125, 206.253.225.12) • Port: Gibt den Port des Proxy-Servers an. • Authentifizierung ermöglichen: Aktivieren Sie diese Option, wenn Sie die Authentifizierung von Lotus Protector for Mail Security gegenüber dem Proxy-Server festlegen möchten. Geben Sie in diesem Fall die Benutzer-ID und das Kennwort ein. • Benutzer-ID/Kennwort: Gibt die Benutzer-ID und das Kennwort zur Authentifizierung an.
Automatische Suche nach Updates	Gibt die Häufigkeit an, mit der Lotus Protector for Mail Security eine Verbindung zu dem Aktualisierungsserver herstellen und nach Updates suchen soll: • Täglich oder wöchentlich nach Updates suchen: Gibt den Wochentag und die Uhrzeit an. Anmerkung: Stellen Sie sicher, dass Lotus Protector for Mail Security mindestens eine Stunde vor automatischen Installationen nach Updates sucht, damit ausreichend Zeit für das Herunterladen der Updates bleibt. • In bestimmten Intervallen nach Updates suchen: Gibt ein Intervall (in Minuten) an. Anmerkung: Der Intervallbereich liegt zwischen 60 Minuten und 1440 Minuten (24 Stunden).

Option	Bezeichnung
Aktualisierung von Sicherheitsinformationen	Gibt an, wie Lotus Protector for Mail Security verfügbare Sicherheitsupdates verarbeiten soll: • Automatischer Download: Legt fest, dass Lotus Protector for Mail Security alle gefundenen Updates herunterladen soll. • Automatische Installation: Legt fest, dass Lotus Protector for Mail Security die heruntergeladenen Updates automatisch installieren soll.
Updates der E-Mail-Sicherheitsdatenbank	Enthält die aktuellsten Spamsignaturen und -heuristiken für die Datenbank von Lotus Protector for Mail Security.
Firmware-Updates	Enthält ein Update des Download Centers, das Folgendes einschließt: • Neue Programmdateien • Korrekturen oder Patch-Codes • Erweiterungen • Onlinehilfe Anmerkung: Einige Firmware-Updates erfordern nach der Installation den Warmstart von Lotus Protector for Mail Security.
Installationsoptionen: Vor der Installation eine vollständige Systemsicherung durchführen.	Diese Option ist standardmäßig aktiviert. Es wird empfohlen, vor der Installation eines Firmware-Updates eine vollständige Systemsicherung durchzuführen. Lotus Protector for Mail Security speichert jeweils nur eine Systemsicherung. Darum wird bei dieser Option die vorherige Systemsicherung überschrieben. • Nicht installieren: Diese Option erfordert die manuelle Installation. Mit dieser Option haben Sie die größte Kontrolle über die Auswirkungen einer Installation auf Ihren Systembetrieb. • Updates automatisch installieren: Die Updates werden automatisch entsprechend der von Ihnen getroffenen Auswahl des Installationszeitpunkts installiert: – Verzögert: Bestimmt den Wochentag und die Uhrzeit der Installation – Sofort: Startet die Installation unverzüglich nach dem Herunterladen des Updates. Mit dieser Option haben Sie die geringste Kontrolle und Vorhersagbarkeit über den Zeitpunkt einer Installation. Achtung: Während der Installation des Updates ist das System möglicherweise offline.

Ereignisbenachrichtigung für Updates konfigurieren

Dieser Abschnitt beschreibt die Vorgehensweise bei der Konfiguration von Lotus Protector for Mail Security, um Sie über Updates zu benachrichtigen.

Vorgehensweise

1. Klicken Sie im Navigationsfenster auf **Updates > Automatische Updates**.
2. Klicken Sie auf die Registerkarte **Ereignisbenachrichtigung**.
3. Stellen Sie folgende Informationen bereit:

Option	Bezeichnung
Statusmeldungen-Protokoll für verfügbare Updates	Benachrichtigt Sie, wenn Updates zum Herunterladen und Installieren bereitstehen.
Statusmeldungen-Protokoll für Aktualisierungsinstallationen	Benachrichtigt Sie, wenn Updates installiert wurden.
Statusmeldungen-Protokoll für Aktualisierungsfehler	Benachrichtigt Sie bei Fehlern, die während der Installation eines Updates aufgetreten sind.
Zustellung der Benachrichtigung	Legt fest, wie die Ereignisbenachrichtigung und Nachrichtenübermittlung aktiviert werden: • E-Mail aktiviert: Legt fest, ob E-Mails für die ausgewählte Nachrichtenstufe aktiviert werden • E-Mail-Name: Gibt den Standard-E-Mail-Namen für die ausgewählte Nachrichtenstufe an • E-Mail konfigurieren: Ermöglicht die Konfiguration von E-Mail-Einstellungen für die ausgewählte Nachrichtenstufe • SNMP-Trap aktiviert: Legt fest, ob SNMP-Trap für die ausgewählte Nachrichtenstufe aktiviert wird. • SNMP konfigurieren: Ermöglicht die Konfiguration von SNMP-Einstellungen für die ausgewählte Nachrichtenstufe.

Erweiterte Parameter für automatische Updates konfigurieren

Dieser Abschnitt beschreibt die Vorgehensweise bei der Konfiguration von erweiterten Parametern, um Leistungsprobleme zu diagnostizieren, zu korrigieren oder zu verbessern, die im Zusammenhang mit der Ausführung von Updates für Lotus Protector for Mail Security auftreten können.

Vorgehensweise

1. Klicken Sie im Navigationsfenster auf **Updates > Automatische Updates**.
2. Klicken Sie auf die Registerkarte **Erweiterte Einstellungen**.
3. Wird der Parameter, den Sie bearbeiten möchten, in der Registerkarte **Erweiterte Einstellungen** nicht angezeigt, führen Sie die folgenden Schritte aus:
 - a. Klicken Sie auf das Symbol **Hinzufügen**.
 - b. Geben Sie den Namen des Parameters ein.
 - c. Geben Sie eine Beschreibung des Parameters ein.
 - d. Geben Sie den Wertetyp und den Wert des Parameters ein.
4. Wird der Parameter, den Sie bearbeiten wollen, bereits in der Registerkarte **Erweiterte Einstellungen** angezeigt, klicken Sie auf den Wert oder die Beschreibung und ändern Sie die Einstellung.

Achtung: In den meisten Fällen müssen Sie die erweiterten Parameter nicht ändern. Ändern Sie diese Parameter nur, wenn Sie vom technischen Support von IBM dazu aufgefordert werden.

Name und Beschreibung	Standardwert
update.disable.remote.discovery Markieren Sie diese Einstellung, um die Fernerkennung von Aktualisierungsdateien vom konfigurierten Downloadserver auszuschalten.	False
update.preserve.update.files Markieren Sie diese Einstellung, um festzulegen, dass Aktualisierungspaketdateien nach erfolgreicher Installation nicht gelöscht werden sollen.	False

5. Klicken Sie auf **OK** und anschließend auf **Änderungen speichern**.

Anhang A. Endbenutzerschnittstelle

In diesem Anhang wird beschrieben, wie ein Administrator Benutzeraccounts und Zugriffsberechtigungen für die Endbenutzerschnittstelle einrichten kann.

Zugriffsberechtigungen für die Endbenutzerschnittstelle einrichten

In diesem Abschnitt wird erläutert, wie Sie die Zugriffsberechtigungen für die Endbenutzerschnittstelle einrichten, damit Benutzer E-Mail-Nachrichten in Quarantäne suchen und anzeigen, persönliche Blockierlisten und persönliche Zulassungslisten verwalten oder ihre täglichen Quarantäneberichte generieren und zustellen können.

Informationen zu diesem Vorgang

Sie können entweder die volle Berechtigung für die Endbenutzerschnittstelle erteilen, indem Sie die Option **Standardzugriffsmodus** auf *Gewährt* festlegen, oder eine differenziertere Konfiguration durch Hinzufügen von Who-Objekten zur Liste erstellen. Der Standardzugriffsmodus wird für alle Benutzer angewendet, die nicht durch Who-Objekte in der Liste dargestellt werden.

Achtung: Wenn Sie die Endbenutzerschnittstelle verwenden möchten, muss der Zugriff auf die Endbenutzerschnittstelle von Lotus Protector for Mail Security auf der Firewallseite entsprechend ermöglicht werden.

Vorgehensweise

1. Klicken Sie im Navigationsfenster auf **Mail Security > Richtlinie**.
2. Klicken Sie auf die Registerkarte **Endbenutzerschnittstelle**.
3. Geben Sie folgende Informationen ein:

Option	Bezeichnung
Standardzugriffsmodus	Gibt den Zugriffsmodus für Benutzer an, die von keinem Who-Objekt auf der Zugriffsliste repräsentiert werden: • Gewährt: Benutzer, die von keinem der Who-Objekte repräsentiert werden, haben die Zugriffsberechtigung auf die Endbenutzerschnittstelle. • Verweigert: Der Zugriff wird den Benutzern verweigert, die von keinem der Who-Objekte auf der Liste repräsentiert werden.

Option	Bezeichnung
Endbenutzerschnittstelle-URL	Stellt die URL-Adresse einer Website bereit, auf die Benutzer zugreifen können, um die Endbenutzerschnittstelle zu verwenden. Diese URL wird auch in den Quarantäneberichten verwendet. Sie können einen Hostnamen oder eine IP-Adresse eingeben. Der Eintrag muss allerdings mit https:// beginnen. Beispiel: https://<Hostname>:4443 Anmerkung: Eine Änderung des Ports für diese URL bewirkt keine Änderung des Empfangsports des internen Web-Servers. Möglicherweise ist eine Änderung dieses Ports erforderlich, wenn Sie einen benutzerdefinierten Port als Standardport in der Firewall verwenden. Achtung: Stellen Sie sicher, dass der angegebene Hostname, der entweder durch ein Makro oder manuell eingegeben wurde, in Ihrer Netzumgebung aufgelöst werden kann.
Who	Gibt an, dass ein bestimmter Benutzer oder eine bestimmte Gruppe, repräsentiert durch ein Who-Objekt, über einen speziellen Zugriffsmodus verfügt.
Zugriffstyp	Gibt den Zugriffstyp für ein bestimmtes Who-Objekt an: • Gewährt: Benutzer, die durch das Who-Objekt repräsentiert werden, haben Zugriff auf die Endbenutzerschnittstelle. • Verweigert: Der Zugriff wird den Benutzern verweigert, die durch das Who-Objekt repräsentiert werden.

4. Klicken Sie auf **OK** und anschließend auf **Änderungen speichern**. Der Eintrag wird in der Liste angezeigt.

Benutzeraccounts für Endbenutzerschnittstelle verwalten

Dieser Abschnitt beschreibt, wie Sie auf der Endbenutzerschnittstelle nach einem Benutzernamen suchen, eine Blockierliste oder eine Zulassungsliste für einen Benutzer von der Endbenutzerschnittstelle löschen, einen Benutzer aus der Verwaltung für Blockier- oder Zulassungslisten auf der Endbenutzerschnittstelle löschen oder das Kennwort eines Benutzers zurückzusetzen und den Zugriff auf die Endbenutzerschnittstelle erneut ermöglichen.

Tabelle 29. Tasks der Endbenutzerschnittstelle

Schaltfläche	Beschreibung
Filter	Sucht auf der Endbenutzerschnittstelle nach einem Benutzer.
Blockierliste/Zulassungsliste löschen	Löscht eine Blockierliste oder eine Zulassungsliste für einen Benutzer auf der Endbenutzerschnittstelle.
Benutzer löschen	Löscht einen Benutzer aus der Verwaltung für eine Blockierliste oder eine Zulassungsliste auf der Endbenutzerschnittstelle.
Kennwort zurücksetzen	Setzt das Kennwort eines Benutzers zurück und ermöglicht den Zugriff auf Endbenutzerschnittstelle. Das neue Kennwort wird automatisch per E-Mail-Nachricht an den entsprechenden Benutzer gesendet.

Erweiterte Parameter für die Endbenutzerschnittstelle konfigurieren

In diesem Abschnitt wird erläutert, wie Sie erweiterte Parameter verwenden, mit denen Sie Leistungsprobleme diagnostizieren, korrigieren oder verbessern können, die im Zusammenhang mit der Endbenutzerschnittstelle auftreten können.

Vorgehensweise

1. Klicken Sie im Navigationsfenster auf **Mail Security > Richtlinie**.
2. Klicken Sie auf die Registerkarte **Erweiterte Einstellungen**.
3. Führen Sie die nachfolgenden Schritte aus, wenn der Parameter, den Sie optimieren möchten, nicht auf der Registerkarte **Erweiterte Einstellungen** angezeigt wird:
 - a. Klicken Sie auf das Symbol **Hinzufügen**.
 - b. Geben Sie den Namen des Parameters ein.
 - c. Geben Sie eine Beschreibung des Parameters ein.
 - d. Geben Sie den Werttyp und den Wert des Parameters ein.
4. Klicken Sie auf das Wert- oder auf das Beschreibungsfeld und ändern Sie die Einstellung, wenn der Parameter, den Sie optimieren möchten, bereits auf der Registerkarte **Erweiterte Einstellungen** angezeigt wird.

Achtung: In den meisten Fällen müssen Sie die erweiterten Parameter nicht ändern. Ändern Sie diese Parameter nur, wenn Sie vom technischen Support von IBM dazu aufgefordert werden.

Name und Beschreibung	Standardwert
clientconnections.count Die Standardanzahl der Clientverbindungen, die zur gleichen Zeit von Benutzern verwendet werden können, um auf die Endbenutzerschnittstelle zuzugreifen.	4

5. Klicken Sie auf **OK**.

Anhang B. Mail Security-Cluster

In diesem Anhang wird beschrieben, wie ein Cluster von Mail Security-Systemen verwaltet wird, der eine Richtlinienverwaltung über mehrere Systeme verteilt.

Informationen zu Mail Security-Clustern

Ein Mail Security-Cluster besteht aus verschiedenen Lotus Protector for Mail Security-Systemen (oder virtuellen Systemen, die auf einem VMware ESX-Server ausgeführt werden), von denen eins die Funktion eines zentralen Systems übernimmt (*Cluster Central*), während die anderen Systeme Clients des zentralen Systems (*Cluster Clients*) sind.

Informationen zu Mail Security-Clustern

Ein Mail Security-Cluster besteht aus einer Anzahl von Systemen (oder virtuellen Systemen, die auf einem VMware ESX-Server ausgeführt werden), von denen eines die Funktion eines zentralen Systems übernimmt (*Cluster Central*), während die anderen Systeme Clients des zentralen Systems (*Cluster Clients*) sind.

Wie werden Daten im Mail Security-Cluster verarbeitet?

Alle Member des Mail Security-Clusters nutzen gemeinsam die Richtlinienkonfigurationseinstellungen des zentralen Systems. Die Richtlinienkonfigurationseinstellungen für das zentrale System werden auf den Seiten **Mail Security-Richtlinie** (Mail Security > Richtlinie) und **Mail Security-Richtlinienobjekte** (Mail Security > Richtlinienobjekte) definiert.

Das zentrale System übernimmt die Funktion des zentralen Datenbankservers für den Mail Security-Cluster. Jedes System im Mail Security-Cluster verfügt über eine lokale Datenbank, in der alle Informationen für die E-Mail-Nachrichten gespeichert werden, die in diesem bestimmten System verarbeitet wurden. Alle Systeme im Mail Security-Cluster replizieren Datenbankveränderungen (z. B. neue Daten, veränderte Daten oder gelöschte Daten) von ihrer lokalen Datenbank in die Datenbank für das zentrale System. Die vom zentralen System verwendete Datenbank erfasst diese Daten, damit die Benutzer ihre Quarantänespeicher durchsuchen und Quarantäneberichte erstellen und an andere Benutzer senden können.

Durch den Cluster verwaltete und replizierte Einstellungen

- Mail Security > Richtlinie
- Mail Security > Richtlinienobjekte

Einige SMTP-Einstellungen beziehen sich auf die unter "Mail Security" definierten Richtlinienobjekte. Richtlinienobjekte werden zwischen den Cluster-Membren repliziert, SMTP-Einstellungen dagegen werden nicht repliziert. Entfernen Sie alle Verweise auf Richtlinienobjekte aus SMTP > Konfiguration > Empfangender SMTP > Empfängerüberprüfung. Stellen Sie nach Einrichten des Clusters sicher, dass Sie die Empfängerüberprüfung erneut aktivieren.

- Mail Security > Berichterstellung
- Beim System registrierte Endbenutzer
- Listeneinträge blockieren und zulassen (unabhängig davon, ob ein LDAP-Verzeichnisbenutzer oder ein "lokaler" Benutzer existiert, der nur in den Systemen vorhanden ist)
- Alle Cluster-Clients replizieren die Daten ihres Quarantäneberichts in die Clusterzentrale. Anschließend generiert die Clusterzentrale die Quarantäneberichte. Die Benutzer erhalten nur einen einzigen Quarantänebericht, der alle unter Quarantäne gestellten E-Mail-Nachrichten enthält, unabhängig davon, welches System die E-Mail-Nachrichten verarbeitet hat.

- Mail Security > E-Mail-Browser (Nachrichtenspeicherdaten werden nicht mehr repliziert.) Beim Durchsuchen des Nachrichtenspeichers wird die Suchabfrage an alle Hosts im Cluster verteilt. Die Ergebnisse werden in einer einzelnen Ansicht (beispielsweise Peer-to-Peer-Suche) kombiniert.

Lokal durch Mitglieder des Clusters (Cluster-Clients) verwaltete Einstellungen

- SMTP-Einstellungen
- TLS-Zertifikate
- Firewall-einstellungen
- IPS-Einstellungen
- Netzeinstellungen
- Routing
- Einstellungen aktualisieren
- Lizenzschlüssel
- Sicherungen

Neuen Mail Security-Cluster erstellen

Verwenden Sie die Seite **Clustering**, um einen Cluster aus Mail Security-Systemen zu erstellen, die Richtlinienverwaltung über mehrere Systeme verteilen.

Informationen zu diesem Vorgang

Beim Erstellen eines Mail Security-Clusters:

- Verliert das System alle aktuellen Daten einschließlich der E-Mail-Nachrichten.
- Alle Verweise auf Zeitplanobjekte (Mail Security > Richtlinienobjekte > Zeitpläne) und FTP-Serverobjekte (Mail Security > Richtlinienobjekte > FTP-Server) müssen entfernt werden.

Vorgehensweise

1. Klicken Sie im Navigationsfenster auf **Mail Security > Clustering**.
2. Klicken Sie auf **Neuen Cluster erstellen** und auf **Weiter**.

Achtung: Die folgenden Konfigurationseinstellungen werden während der Erstellung des Clusters automatisch auf das System angewendet:

- Firewall-Ports 5432 (Datenbankzugriff) und 4990 (Clusterkommunikation) werden geöffnet, um die Kommunikation zwischen dem zentralen System und dem System zu ermöglichen, das dem -Cluster hinzugefügt werden soll.
- Der Netzzeitserver wird aktiviert, um die Zeiteinstellungen für alle Mitglieder des Mail Security-Clusters zu synchronisieren.

3. Im Abschnitt **Neue Clustereinstellungen**:

- a. Geben Sie die Kennphrase für den Mail Security-Cluster ein und bestätigen Sie diese.

Achtung: Verwenden Sie eine Kennphrase, die Sie sich gut merken können. Das Zurücksetzen oder Wiederherstellen der Kennphrase nach ihrer Erstellung durch IBM ist nicht möglich.

- b. Wählen Sie eine IP-Adresse aus der Liste der **Kommunikations-IPs** aus und klicken Sie auf **Weiter**.

4. Nach Erfassen aller Details klicken Sie auf **Weiter**, um den Prozess zum Erstellen des Clusters zu starten.

Wichtig: Während des Erstellens des Clusters verliert das System alle aktuellen Daten einschließlich der E-Mail-Nachrichten. Sie können auf die Services auf dem System erst wieder zugreifen, nachdem der Vorgang zum Erstellen der Cluster abgeschlossen wurde.

Mit vorhandenem Mail Security-Cluster verbinden

Verwenden Sie die Seite **Clustering**, um das System einem vorhandenen Mail Security-Cluster hinzuzufügen, wenn Sie die Arbeitslast auf mehrere Maschinen verteilen möchten.

Informationen zu diesem Vorgang

Wenn ein System mit einem vorhandenen Mail Security-Cluster verbunden wird:

- Verliert das System alle aktuellen Daten einschließlich der E-Mail-Nachrichten.
- Alle Verweise auf Zeitplanobjekte (Mail Security-Richtlinienobjekte und Zeitpläne) und FTP-Serverobjekte (Mail Security-Richtlinienobjekte und FTP-Server) müssen entfernt werden.

Vorgehensweise

1. Klicken Sie im Navigationsfenster auf **Mail Security > Clustering**.

2. Klicken Sie auf **Mit vorhandenem Cluster verbinden** und auf **Weiter**.

Achtung: Die folgenden Konfigurationseinstellungen werden automatisch auf ein System angewendet, das mit dem Cluster verbunden wird:

- Firewall-Ports 5432 (Datenbankzugriff) und 4990 (Clusterkommunikation) werden geöffnet, um die Kommunikation zwischen dem zentralen System und dem System zu ermöglichen, das dem -Cluster hinzugefügt werden soll.
- Der Netzzeitserver wird aktiviert, um die Zeiteinstellungen für alle Mitglieder des Mail Security-Clusters zu synchronisieren.
- Alle Who-Objekte werden von der SMTP-Empfängerüberprüfung entfernt.
- Die Sicherung der FTP-Protokolldatei wird inaktiviert.

3. Im Abschnitt **Clusterverbindungsdetails**:

- a. Geben Sie die IP-Adresse des zentralen Systems für den Mail Security-Cluster ein.
- b. Geben Sie die Kennphrase für den Mail Security-Cluster ein und bestätigen Sie diese.
- c. Wählen Sie eine IP-Adresse für das System aus, das über die Liste **Kommunikations-IPs** verbunden wird und klicken Sie auf **Weiter**.

4. Klicken Sie auf **Weiter**, um den Vorgang zum Verbinden mit dem Cluster zu starten.

Um die Verbindungsparameter für die Datenbank des zentralen Systems zu empfangen, werden folgende Schritte vom System durchgeführt:

- a. Die Verarbeitung von E-Mail-Nachrichten wird abgebrochen, einschließlich des SMTP-Servers.
- b. Es wird eine Verbindung mit der Datenbank des zentralen Systems hergestellt.
- c. Alle Daten aus der eigenen Datenbank werden entfernt.
- d. Alle Konfigurationsdaten aus dem zentralen System (*Clusterzentrale*) werden in die eigene Datenbank repliziert.
- e. Die zuvor gelesene Richtlinie aus der Datenbank des zentralen Systems wird angewendet.
- f. Die Verarbeitung von E-Mail-Nachrichten wird gestartet.

Kennphrasen oder IP-Adressen für den Mail Security-Cluster ändern

In diesem Abschnitt wird erklärt, wie Sie die Kennphrase für das zentrale System im Mail Security-Cluster oder die IP-Adresse eines Systems im Mail Security-Cluster ändern können.

Vorgehensweise

1. Klicken Sie im Navigationsfenster auf **Mail Security > Clustering**.
2. Klicken Sie auf **Diesen Cluster verwalten**.
3. Wählen Sie eine Option aus:

Wenn Sie folgende Aktion ausführen möchten...	Dann...
Kennphrase für das primäre zentrale System im Cluster ändern	1. Wechseln Sie zum System <i>Clusterzentrale</i> und klicken Sie auf Cluster-Kennphrase ändern. 2. Geben Sie die aktuelle Kennphrase für den Mail Security-Cluster ein. Geben Sie anschließend zweimal die neue Kennphrase ein, um sie zu bestätigen. 3. Klicken Sie auf Kennphrase ändern.
IP-Adresse eines Systems im Cluster ändern	1. Wählen Sie ein System aus und klicken Sie auf IP-Adresse aktualisieren. 2. Geben Sie die Kennphrase für den Mail Security-Cluster ein und stellen Sie anschließend eine neue IP-Adresse zur Verfügung. 3. Klicken Sie auf IP-Adresse ändern.

Client aus dem Mail Security-Cluster entfernen

In diesem Abschnitt wird erläutert, wie Sie einen Client aus einem Mail Security-Cluster entfernen.

Vorgehensweise

1. Klicken Sie im Navigationsfenster auf **Mail Security > Clustering**.
2. Klicken Sie auf **Diesen Cluster verwalten**.
3. Wählen Sie den Client aus, der aus dem Mail Security-Cluster entfernt werden soll.
4. Geben Sie die Kennphrase für den Mail Security-Cluster ein.

Anmerkung: Hierbei handelt es sich um die Kennphrase, die von Ihnen oder einem anderen Administrator beim Erstellen des Mail Security-Clusters festgelegt wurde.

5. Klicken Sie auf **Diesen Client entfernen**. Der Client stoppt die Verarbeitung von SMTP-Datenverkehr und verlässt den Mail Security-Cluster.
6. Starten Sie die Verarbeitung des SMTP-Datenverkehrs neu.

Cluster von Mail Security-Systemen löschen

In diesem Abschnitt wird erläutert, wie Sie einen Cluster von Mail Security-Systemen wieder an ein einzelnes System zurückgeben.

Vorgehensweise

1. Klicken Sie im Navigationsfenster auf **Mail Security > Clustering**.
2. Klicken Sie auf der Seite **Clusterzentralenmodus** auf **Diesen Cluster löschen**.
3. Geben Sie die Kennphrase für den Mail Security-Cluster ein und wählen Sie anschließend das Löschen des Clusters aus.

Anhang C. Integration in Lotus Domino

In diesem Anhang wird beschrieben, wie Sie Lotus Protector for Mail Security (Version 2.5 oder höher) in Ihre vorhandene Infrastruktur von Lotus Domino und Notes (Version 8.5.1 oder höher) integrieren.

Serverkonfiguration für Lotus Domino

Sie müssen Einstellungen in den Richtlinien des Domino-Administratordesktops angeben, die es Lotus Protector for Mail Security ermöglichen, die Funktionen zum Spamschutz in Lotus Notes-Clients zu integrieren. Alle Schutzfunktionen sind verfügbar, wenn der Lotus Notes-Client die Lotus Domino-Richtlinie empfängt.

Richtlinie des Domino-Administratordesktops konfigurieren, um die Integration zu ermöglichen

Verwenden Sie die Einstellung \$PROTECTOR_LOCATION in der Datei NOTES.INI, um die Speicherposition der Adresse anzugeben, die Sie für den Zugriff auf Lotus Protector for Mail Security verwenden sollten.

Vorgehensweise

1. Klicken Sie im Dokument mit den Richtlinieneinstellungen des Domino-Administratordesktops auf die Registerkarte **Benutzerdefinierte Einstellungen - Notes.ini**.
2. Klicken Sie auf **Liste bearbeiten**.
3. Füllen Sie die folgenden Felder aus:

Option	Bezeichnung
Element	Geben Sie \$PROTECTOR_LOCATION an.
Wert	Geben Sie die Adresse für Lotus Protector for Mail Security in einem der folgenden Formate an: • Adresse:Port (Beispiel: protector1.mycompany.com:4443) • IP:Port (Beispiel: 192.168.2.42:4443) Anmerkung: Für Lotus Protector for Mail Security wird normalerweise der Port 4443 verwendet. Der Verbindungsport unterscheidet sich möglicherweise, wenn Sie NAT als Teil Ihrer Netzkonfiguration verwenden.
Erzwingen	Klicken Sie auf dieses Kontrollkästchen, wenn Sie die Richtlinieneinstellung erzwingen möchten. Wenn Sie die Richtlinie erzwingen, überschreibt sie Einstellungen, die Vorrang vor dieser Einstellung haben (einschließlich der Einstellungen, die über eine explizite Richtlinie zugeordnet wurden).

4. Speichern und schließen Sie das Dokument mit den Richtlinieneinstellungen.

Nächste Schritte

Konfigurieren Sie Einstellungen in Lotus Protector for Mail Security, um die Integration auf dem Lotus Domino-Server zu ermöglichen.

Konfiguration von Lotus Protector for Mail Security

In diesem Abschnitt wird erläutert, wie Sie Zugriffsberechtigungen und die Benutzerauthentifizierung in Lotus Protector for Mail Security aktivieren, die für die Integration auf dem Lotus Domino-Server erforderlich sind.

Vorbereitende Schritte: Sie müssen ein Lotus Protector for Mail Security-System haben, das bereits online ist und den E-Mail-Verkehr filtert. Der Administrator für Lotus Protector for Mail Security muss bei Lotus Protector Manager angemeldet sein.

Zugriffsberechtigungen für Lotus Notes-Benutzer aktivieren

In diesem Abschnitt wird erläutert, wie Sie Zugriffsberechtigungen einrichten, damit Lotus Notes-Benutzer blockierte E-Mail-Nachrichten suchen und anzeigen, persönliche Blockierlisten und persönliche Zulassungslisten verwalten oder ihre täglichen Quarantäneberichte generieren und zustellen können.

Ports der lokalen Firewall öffnen

Sie müssen sicherstellen, dass Lotus Protector for Mail Security eine Verbindung zu TCP-Port 4443 herstellen kann, damit Lotus Notes-Benutzer auf die Endbenutzerschnittstelle zugreifen können.

Vorgehensweise

1. Klicken Sie im Navigationsfenster auf **System > Firewall**.
2. Aktivieren Sie die Schnittstelle (normalerweise eth1), die mit Ihrem internen Netz verbunden ist, im Abschnitt "Endbenutzerzugriff (4443)".
3. Speichern Sie Ihre Änderungen.

Einrichten der Zugriffsberechtigungen für die Endbenutzerschnittstelle

Sie müssen Zugriffsberechtigungen für die Endbenutzerschnittstelle einrichten, damit Lotus Notes-Benutzer blockierte E-Mail-Nachrichten suchen und anzeigen, persönliche Blockierlisten und persönliche Zulassungslisten verwalten und ihre täglichen Quarantäneberichte generieren und zustellen können.

Vorgehensweise

1. Klicken Sie im Navigationsfenster auf **E-Mail-Sicherheit > Richtlinie**.
2. Klicken Sie auf die Registerkarte **Endbenutzerschnittstelle**.
3. Setzen Sie **Standardzugriffsmodus** auf *Gewährt*.
4. Speichern Sie Ihre Änderungen.

Benutzerauthentifizierung über Ihren Lotus Domino-Server aktivieren

Sie müssen Ihren Lotus Domino-Server in Lotus Protector for Mail Security registrieren, damit Ihre Benutzer sich mithilfe Ihres Domino-Servers authentifizieren können. Lotus Protector for Mail Security kommuniziert mithilfe von LDAP mit dem Domino-Server. Wenn für den LDAP-Zugriff auf Ihren Domino-Server Authentifizierung erforderlich ist, müssen Sie die entsprechenden Anmeldeberechtigungsnachweise bereitstellen.

Einrichten der Verbindung zum Lotus Domino-Server Vorgehensweise

1. Klicken Sie im Navigationsfenster auf **Mail Security > Richtlinienobjekte**.
2. Klicken Sie auf die Registerkarte **Verzeichnisse**.
3. Suchen Sie den Eintrag für die Domino-Beispieldomäne in der Verzeichnisliste.
4. Aktivieren Sie das Kontrollkästchen **Aktiv** neben diesem Eintrag.
5. Klicken Sie auf das Symbol **Bearbeiten**.
6. Klicken Sie auf die Registerkarte **LDAP-Server**.
7. Geben Sie den Hostnamen oder die IP-Adresse Ihres Domino-Servers in das Feld **Host** ein.
8. Geben Sie den Benutzernamen des Benutzers, der die entsprechenden Zugriffsberechtigungen zum Lesen des Domino-LDAP hat, in das Feld **Benutzername** ein.
9. Klicken Sie auf **Kennwort eingeben** und geben Sie anschließend das Kennwort für den LDAP-Benutzer ein, den Sie im Feld **Benutzername** angegeben haben.
10. Klicken Sie auf **OK** und speichern Sie anschließend Ihre Änderungen.

Anmerkung: Auch wenn ein Domino-Server der bevorzugte Verzeichnisservers für die Benutzerauthentifizierung ist, können Sie die meisten mit LDAP kompatiblen Verzeichnisservers verwenden. Dies ist beispielsweise hilfreich, wenn Sie Microsoft Active Directory für die Benutzerauthentifizierung verwenden.

Fehlerbehebung für die LDAP-Verbindung zu Ihrem Lotus Domino-Server

Die meisten Probleme bei der LDAP-Verzeichnisintegration treten aufgrund eines falschen LDAP-Benutzernamens oder eines falschen LDAP-Kennworts auf. Sie können das Ereignisprotokoll in Lotus Protector Manager überprüfen, um zu ermitteln, ob Lotus Protector for Mail Security eine Verbindung mit dem LDAP-Server für Lotus Domino hergestellt hat. Möglicherweise sehen Sie jedoch keine LDAP-spezifischen Ereignisse, bis ein Benutzer versucht hat, sich über Lotus Domino zu authentifizieren.

Vorgehensweise

1. Klicken Sie im Navigationsfenster auf **System > Ereignis**.
2. Suchen Sie im Ereignisprotokoll nach Fehlern, die möglicherweise darauf hinweisen, dass Probleme bei der Herstellung einer Verbindung mit dem LDAP-Server für Lotus Domino aufgetreten sind.

Anhang D. Erweiterte Parameter

In diesem Anhang werden die erweiterten Parameter für Lotus Protector for Mail Security beschrieben, mit denen Sie Leistungsprobleme diagnostizieren, korrigieren oder verbessern können, die in Ihrem Netz oder in Ihrer Umgebung auftreten können.

Wichtig: Ändern Sie diese Parameter nur, wenn Sie dazu vom technischen Support von IBM aufgefordert werden.

Allgemeine erweiterte Parameter

In diesem Abschnitt werden einige der gebräuchlicheren Parameter für Lotus Protector for Mail Security definiert.

Tabelle 30. Allgemeine erweiterte Parameter

Name und Beschreibung	Standardwert
log_level Aktiviert oder deaktiviert die Ausgabe von E-Mail-Nachrichten. Gültige Werte sind 0 (keine Protokollausgabe) bis 4 (detaillierte Protokollausgabe).	0
recipient.nospam_learn Gibt die Empfänger-E-Mail-Adresse für den Collector von E-Mails an, die kein Spam sind.	notspam@kassel.ibm.com
recipient.spam_learn Gibt die Empfänger-E-Mail-Adresse für den Collector von E-Mails an, die Spam sind.	spam@kassel.ibm.com
sendmail.includetrackingdata Wenn dieser Parameter auf <i>true</i> festgelegt ist, werden Nachrichtenverfolgungsinformationen an E-Mail-Nachrichten angehängt, die an nospam_learn und spam_learn gesendet werden.	True
display_mailbody.disable Wenn dieser Parameter auf <i>true</i> festgelegt ist, wird der Haupttext einer E-Mail-Nachricht nicht vom Browser des Nachrichtenspeichers angezeigt.	False
Ressourcenüberwachung	
operational.behaviour Passt die Schwellenwerte für das Erreichen der Arbeitsspeicher- und Plattenspeicherwarnstufen bei 1 und 2 an. 0 = Die Software kann weniger Arbeitsspeicher oder Plattenspeicher als normal verwenden, bis die Warnstufen erreicht sind. 1 = Normales Verhalten 2 = Die Software kann mehr Arbeitsspeicher oder Plattenspeicher als normal verwenden, bis die Warnstufen erreicht sind. 3 = Ein besonderer Wert für die Deaktivierung der Ressourcenüberwachung. Es wird nicht empfohlen, diesen Wert zu verwenden.	1

Tabelle 30. Allgemeine erweiterte Parameter (Forts.)

Name und Beschreibung	Standardwert
Filterdatenbank	
dbupdates.maxbandwidth Begrenzt die Bandbreite, die für Datenbankaktualisierungen verwendet wird, auf den angegebenen Wert in KB pro Sekunde. Durch den Wert 0 wird die verwendete Bandbreite nicht begrenzt.	0 (KB pro Sekunde)
dbupdates.weblearn Aktiviert den Upload unbekannter URLs für den Download-Server.	False

Erweiterte Parameter für LDAP-Server

In diesem Abschnitt werden die erweiterten Parameter für LDAP-Verzeichnisse definiert, die von Lotus Protector for Mail Security verwendet werden.

Tabelle 31. Erweiterte Parameter für LDAP-Server

Name und Beschreibung	Standardwert
dirservice.connection.timeout Gibt das Zeitlimit für die Socketverbindung an, die für alle LDAP-Server- und NTLM-Clientabfragen verwendet wird. Wenn das Zeitlimit überschritten wird und keine Verbindung hergestellt werden kann, wird der Server als nicht erreichbar gekennzeichnet.	3000 (in Millisekunden)
dirservice.reconnect.interval Legt fest, wie lange ein NTLM-Client oder ein LDAP-Server, die nicht erreichbar sind, in diesem Zustand verbleiben, bis erneut versucht wird, eine Verbindung herzustellen.	180 (in Sekunden)

Erweiterte Parameter für Nachrichtenspeicher

In diesem Abschnitt werden die erweiterten Parameter für die Nachrichtenspeicher definiert, die von Lotus Protector for Mail Security verwendet werden.

Tabelle 32. Erweiterte Parameter für Nachrichtenspeicher

Name und Beschreibung	Standardwert
msgstore.release.tag.subject.disable Wenn dieser Parameter auf <i>false</i> festgelegt ist, werden E-Mail-Nachrichten gekennzeichnet, wenn sie aus einem Quarantänespeicher freigegeben werden. Siehe Parameter msgstore.release.tag.subject.string unten.	False
msgstore.release.tag.subject.string Fügt diese Zeichenfolge am Anfang des Betreffs einer E-Mail-Nachricht hinzu, wenn die Nachricht aus einem Quarantänespeicher freigegeben wird. Siehe Parameter msgstore.release.tag.subject.disable oben.	[Aus Quarantäne freigegeben]
nospam.send.to.recipients Wenn dieser Parameter auf <i>true</i> festgelegt ist, wird eine E-Mail-Nachricht, die an <code>notspam@kassel.ibm.com</code> gesendet wurde, auch an den/die ursprünglichen Empfänger gesendet.	False
quarantinereport.maxlines Gibt die maximale Anzahl der E-Mail-Nachrichten an, die in einem Quarantänebericht aufgelistet werden können.	100
msgstore.quarantine_domains Gibt eine durch Semikolons getrennte Liste von SMTP-Domänen an, für die eine Quarantäne zulässig ist, zusätzlich zu den lokalen SMTP-Domänen.	

Erweiterte Parameter für SMTP-Einstellungen

In diesem Abschnitt werden die erweiterten Parameter für die SMTP-Einstellungen definiert, die von Lotus Protector for Mail Security verwendet werden.

Tabelle 33. Erweiterte Parameter für SMTP-Einstellungen

Name und Beschreibung	Standardwert
smtp.command_delay Legt die Verzögerung für die einzelnen SMTP-Befehle fest.	0 (in Millisekunden)
smtp.passthrough Wenn dieser Parameter auf <i>true</i> festgelegt ist, werden E-Mail-Nachrichten nicht analysiert, sondern an das nächste SMTP-Relay weitergeleitet.	False
xmail.smtp.threads Gibt die Anzahl der Threads an, die zum Empfangen von E-Mail-Nachrichten verwendet werden.	256
smtp.check_helo_domain Aktiviert die HELO-Domänenprüfung gemäß RFC 2821, Abschnitt 4.1.2.	0
smtp.check_return_path Aktiviert die Prüfung des Return Path (MAIL FROM) gemäß RFC 2821, Abschnitt 4.1.2.	0
smtp.check_forward_path Aktiviert die Prüfung des Weitergabepfads (MAIL FROM) gemäß RFC 2821, Abschnitt 4.1.2.	0
smtp.throttle.unchecked_max_count Legt den errechneten Maximalwert des Füllstands für die Warteschlange "unchecked" fest. Wichtig: Dieser Wert sollte nur geändert werden, wenn es absolut notwendig ist.	10000/5000
smtp.ipc.send_timeout Gibt das Zeitlimit für IPC an, das an den Mail Security-Dämon gesendet wird.	50000 (in Millisekunden)

Erweiterte Parameter für die DNSBL-Einstellungen

In diesem Abschnitt werden die erweiterten Parameter für die DNSBL-Einstellungen (DNS-Blockierliste) definiert.

Tabelle 34. Erweiterte Parameter für die DNSBL-Einstellungen

Name und Beschreibung	Standardwert
dnsblthreads.count Die Mindestanzahl an DNSBL-Threads, die für die DNSBL-Prüfung verwendet werden. Bei Bedarf werden Threads vom Prüfprozess dynamisch bis zum Maximalwert zugeordnet.	20 (Hardware) 10 (VMware)
host_reputation.border_ips Eine durch Semikolons getrennte Liste von DNSBL-Grenz-IP-Adressen.	

Erweiterte Parameter für eine Clusterreplizierung

In diesem Abschnitt werden die erweiterten Parameter für die Replizierung eines Systemclusters definiert.

Tabelle 35. Erweiterte Parameter für Clusterreplikation

Name und Beschreibung	Standardwert
replication.alerting.warn.perc Wenn die Replizierungseinstufung diesen Wert überschreitet, wird eine Warnungs-Statusmeldung generiert.	90
replication.alerting.warn.duration Wenn der Füllstand den warn.perc -Wert über einen längeren Zeitraum als angegeben überschreitet, wird ein Warnungsstatus angewendet.	30*60 (30 Minuten)
replication.alerting.error.perc Wenn die Replizierungseinstufung diesen Wert überschreitet, wird eine Fehler-Statusmeldung generiert.	200
replication.alerting.error.duration Wenn der Füllstand den error.perc -Wert über einen längeren Zeitraum als angegeben überschreitet, wird ein Fehlerstatus angewendet.	60*60 (1 Stunde)
replication.alerting.critical.perc Wenn die Replizierungseinstufung diesen Wert überschreitet, wird das Entfernen des Cluster-Hosts aus dem Cluster erzwungen, um einen Überlauf der Datenbank zu verhindern.	400
replication.alerting.critical.duration Wenn der Füllstand den critical.perc -Wert über einen längeren Zeitraum als angegeben überschreitet, wird ein kritischer Status angewendet.	24*60*60 (1 Tag)

Erweiterte Parameter für die Endbenutzerschnittstelle

In diesem Abschnitt werden die erweiterten Parameter für den Zugriff auf die Endbenutzerschnittstelle definiert.

Tabelle 36. Endbenutzerschnittstelle, erweiterte Parameter

Name und Beschreibung	Standardwert
clientconnections.count Gibt die standardmäßige Anzahl der Clientverbindungen an, die zur gleichen Zeit von Benutzern verwendet werden können, um auf die Endbenutzerschnittstelle zuzugreifen.	4

Anhang E. Die Funktionen zur behindertengerechten Bedienung erfordern Lotus Protector for Mail Security.

Funktionen zur behindertengerechten Bedienung helfen Benutzern mit einer Behinderung, beispielsweise einer eingeschränkten Mobilität oder einem eingeschränkten Sehvermögen, IT-Produkte erfolgreich zu nutzen.

IBM und Barrierefreiheit

Weitere Informationen zum Engagement von IBM für eine behindertengerechte Bedienung finden Sie im *IBM Accessibility Center* unter der Adresse <http://www.ibm.com/able>.

Bemerkungen

Die vorliegenden Informationen wurden für Produkte und Services entwickelt, die auf dem deutschen Markt angeboten werden.

Möglicherweise bietet IBM die in dieser Dokumentation beschriebenen Produkte, Services oder Funktionen in anderen Ländern nicht an. Informationen über die gegenwärtig im jeweiligen Land verfügbaren Produkte und Services sind beim zuständigen IBM Ansprechpartner erhältlich. Hinweise auf IBM Lizenzprogramme oder andere IBM Produkte bedeuten nicht, dass nur Programme, Produkte oder Services von IBM verwendet werden können. Anstelle der IBM Produkte, Programme oder Services können auch andere, ihnen äquivalente Produkte, Programme oder Services verwendet werden, solange diese keine gewerblichen oder anderen Schutzrechte von IBM verletzen. Die Verantwortung für den Betrieb von Produkten, Programmen und Services anderer Anbieter liegt beim Kunden.

Für in diesem Handbuch beschriebene Erzeugnisse und Verfahren kann es IBM Patente oder Patentanmeldungen geben. Mit der Auslieferung dieses Handbuchs ist keine Lizenzierung dieser Patente verbunden. Lizenzanforderungen sind schriftlich an folgende Adresse zu richten (Anfragen an diese Adresse müssen auf Englisch formuliert werden):

IBM Director of Licensing
IBM Europe, Middle East & Africa
Tour Descartes
2, avenue Gambetta
92066 Paris La Defense
France

Trotz sorgfältiger Bearbeitung können technische Ungenauigkeiten oder Druckfehler in dieser Veröffentlichung nicht ausgeschlossen werden. Die hier enthaltenen Informationen werden in regelmäßigen Zeitabständen aktualisiert und als Neuausgabe veröffentlicht. IBM kann ohne weitere Mitteilung jederzeit Verbesserungen und/oder Änderungen an den in dieser Veröffentlichung beschriebenen Produkten und/oder Programmen vornehmen.

Verweise in diesen Informationen auf Websites anderer Anbieter werden lediglich als Service für den Kunden bereitgestellt und stellen keinerlei Billigung des Inhalts dieser Websites dar. Das über diese Websites verfügbare Material ist nicht Bestandteil des Materials für dieses IBM Produkt. Die Verwendung dieser Websites geschieht auf eigene Verantwortung.

Werden an IBM Informationen eingesandt, können diese beliebig verwendet werden, ohne dass eine Verpflichtung gegenüber dem Einsender entsteht.

Lizenznehmer des Programms, die Informationen zu diesem Produkt wünschen mit der Zielsetzung: (i) den Austausch von Informationen zwischen unabhängig voneinander erstellten Programmen und anderen Programmen (einschließlich des vorliegenden Programms) sowie (ii) die gemeinsame Nutzung der ausgetauschten Informationen zu ermöglichen, wenden sich an folgende Adresse:

IBM Corporation
P.O. Box 12195
3039 Cornwallis Road
Research Triangle Park, NC 27709-2195
U.S.A

Die Bereitstellung dieser Informationen kann unter Umständen von bestimmten Bedingungen - in einigen Fällen auch von der Zahlung einer Gebühr - abhängig sein.

Die Lieferung des in diesem Dokument beschriebenen Lizenzprogramms sowie des zugehörigen Lizenzmaterials erfolgt auf der Basis der IBM Rahmenvereinbarung bzw. der Allgemeinen Geschäftsbedingungen von IBM, der IBM Internationalen Nutzungsbedingungen für Programmpakete oder einer äquivalenten Vereinbarung.

Aussagen über Pläne und Absichten von IBM unterliegen Änderungen oder können zurückgenommen werden und repräsentieren nur die Ziele von IBM.

Marken

IBM, das IBM Logo und ibm.com sowie Lotus sind Marken oder eingetragene Marken der International Business Machines Corporation. Weitere Produkt- und Servicenamen können Marken von IBM oder anderen Herstellern sein. Eine aktuelle Liste der IBM Marken finden Sie im Web unter www.ibm.com/legal/copytrade.shtml.

Linux ist eine eingetragene Marke von Linus Torvalds in den USA und/oder anderen Ländern.

UNIX ist eine eingetragene Marke von The Open Group in den USA und anderen Ländern.

Microsoft und Windows sind Marken der Microsoft Corporation in den USA und/oder anderen Ländern.

Weitere Unternehmens-, Produkt- oder Servicenamen können Marken anderer Hersteller sein.

Index

Sonderzeichen

/etc/xmail/logs/ 80
\$PROTECTOR_LOCATION 105
/var/log/messages 80

A

Administratorkennwort 12
Administratormodus 2
Aktion blockieren 47
Aktion fortsetzen 47
Aktion zulassen 47
Analyse der Nullebene 31
 Blockierantwort 32
 Fehlercodes 33
 Fehlernachricht 33
 Headerfeld 32
 Spamkategorie 31
 Unzustellbarkeitsberichte 31
Analyse der Nullebene, Spam 4
Analyse der Nullebene, Unzustellbarkeitsbericht 3
Analyse des Dateianhangs 70
Analysemodul "Absenderblockierliste für Benutzer" 56
Analysemodul "Absenderzulassungsliste für Benutzer" 56
Analysemodul "Anhangprüfung" 53
Analysemodul "Dateityp" 53
Analysemodul "Nachrichtenfeldprüfung" 53
Analysemodul "Phishing-Prüfung" 53
Analysemodul "Schlüsselwortsuche" 53
Analysemodul "Sender Policy Framework" 54
Analysemodul "Spam-Bayes-Klassifikator" 54
Analysemodul "Spam-DNSBL-Prüfung" 55
Analysemodul "Spam-URL-Prüfung" 56
Analysemodul "Spamdatenflussprüfung" 55
Analysemodul "Spamfingerabdruck" 55
Analysemodul "Spamheuristik" 55
Analysemodul "Spamschlüsselwort" 55
Analysemodul "Spamsignaturdatenbank" 56
Analysemodul "Spamstrukturprüfung" 56
Analysemodul "Sprachprüfung" 53
Analysemodul "URL-Prüfung" 56
Analysemodul "Verbund" 53
Analysemodul "Virenprüfung" 56
Analysemodule
 Absenderblockierliste für Benutzer 53
 Absenderzulassungsliste für Benutzer 53
 Anhangprüfung 53
 Dateityp 53

 Analysemodule (*Forts.*)
 Malware-Fernerkennung 53
 Nachrichtenfeldprüfung 53
 Phishing-Prüfung 53
 Schlüsselwortsuche 53
 Spam-Bayes-Klassifikator 53
 Spam-DNSBL-Prüfung 53
 Spam-URL-Prüfung 53
 Spamdatenflussprüfung 53
 Spamfingerabdruck 53
 Spamheuristik 53
 Spamschlüsselwort 53
 Spamsignaturdatenbank 53
 Spamstrukturprüfung 53
 Sprachprüfung 53
 URL-Prüfung 53
 Verbund 53
 Virenprüfung 53
 Virensignaturerkennung 53
Anleitung für IBM Softwareunterstützung ix
Antivirensignaturen 89
Antivirensoftware 56
Antivirenupdates 89
Antiviruslizenz 89
Archivierte E-Mail-Nachrichten 64
Auffangdatei 80
Automatische Updates
 Alertprotokollierung 92
 Ereignisbenachrichtigung konfigurieren 92
 erweiterte Parameter 93
 konfigurieren 90

B

Barrierefreiheit 115
Bayes-Datenbank 54
Bayessches Klassifikationsmerkmal 54
Bedingungen 52
Bedingungsobjekte 52
Befehlszeile ix
Benachrichtigung über Statusmeldungen 75, 77
Bericht zu Top 10-Analysemodulen 81
Bericht zu Top 10-Empfängern 81
Bericht zu Top 10-Responses 81
Bericht zu Top 10-Sendern 81
Bericht zu Top 10-Viren 81
Bericht zu übereinstimmenden Regeln 81
Bericht zur Datenverkehrsüberwachung 81
Bericht zur Kurzübersicht 81
Bericht zur Richtlinienkonfiguration 81
 Datenverkehrsüberwachung 81
 Kurzübersicht 81
 Richtlinienkonfiguration 81
 Top 10-Analysemodule 81
 Top 10-Empfänger 81

Berichte (*Forts.*)
 Top 10-Responses 81
 Top 10-Sender 81
 Top 10-Viren 81
 Typen 81
 Übereinstimmende Regeln 81
Berichterstellung 73
Bewertungsstatus 4
 Arbeitsspeicher- und Plattenbelegung 4
 E-Mail-Analysewarteschlange 4
 E-Mails nicht in Datenbank 4
 Nachrichtenverfolgung 4
 SMTP-Service 4
 Warteschlange für abgehende E-Mail-Nachrichten 4
Blockierliste 29
Blockierliste löschen 97
Blockierte E-Mail-Nachrichten 65
Blockiertes Verzeichnis 35

C

CAL (Content Analysis Library) 7
Cluster 99
 Client entfernen aus 102
 durch Cluster Central verwaltete und replizierte Einstellungen 99
 durch Cluster-Clients verwaltete Einstellungen 100
 entfernen 103
 erstellen 100
 IP-Adresse ändern 102
 Kennphrase ändern 102
 löschen 103
 Mitglied hinzufügen 101
 verbinden 101
Cluster-Clients 99
Clusteringseite 102, 103
Clusterzentrale 99
CPU-Auslastung 5
CSF-Tracedatei 78

D

Dateianhänge
 Inhalte überprüfen 70
 Inhalte untersuchen 70
Datenverkehrsstatus 5
 Durchschnitt ausgehender E-Mails 5
 Durchschnitt eingehender E-Mails 5
 E-Mails in Warteschlange für Analyse 5
 E-Mails in Warteschlange für erneute Zustellung 5
 E-Mails in Warteschlange für Zustellung 5
Datumseinstellungen 13
DER-Format
 für Zertifikate 42

- DFV-Tracedatei 78
- DHCP 15
- Diagnosedatei 80
- Diesen Cluster verwalten 102
- DNS-Einstellungen 15
- DNS-MX-Einträge 19
- DNSBL 29
- DNSBL-Einstellungen, erweiterte Parameter 113
- DNSBL-Listen 71
- DNSBL-Server 55
- DNSBL/Spamdatenfluss 71
- Dokumentation vii
- Domain Name Server Block List 29
- Dynamischer Hostreputationsfilter 33

E

- E-Mail- und SNMP-Statusmeldungen
 - erweiterte Parameter 77
- E-Mail-Adressen
 - definieren 11
- E-Mail-Browser 65
- E-Mail-Datenfluss 55
- E-Mail-Nachrichten
 - erneutes Spoolen 44
 - frozen 65
 - Status von 44
 - unter Quarantäne gestellt 65
 - unzustellbare löschen 38
 - Verfolgung 73
 - verzögert 65
- E-Mail-Sicherheits-Datenbank
 - aktualisieren 10
- E-Mail-Sicherheitslizenz 89
- E-Mail-Sicherheitsrichtlinie 47, 69
 - konfigurieren 47, 69
 - Verarbeitung 47
- E-Mail-Speicher 64
- Einstellungen für die externe Schnittstelle 15
- Empfängerüberprüfung 3, 30, 49, 73
- Endbenutzerschnittstelle 72, 95, 97
 - Benutzer löschen 97
 - Benutzeraccounts verwalten 97
 - Erweiterte Parameter 97, 114
 - Kennwörter zurücksetzen 97
 - Lotus Notes-Zugriffsberechtigungen 106
 - Zugriffs-URL 95
- Ereignisse
 - filtern 79
 - mit hohem Risiko 79
 - mit mittlerem Risiko 79
 - mit niedrigem Risiko 79
 - verwalten 79
- Erweiterte Parameter
 - allgemein 109
 - automatische Updates 93
 - Clusterreplikation 113
 - DNSBL-Einstellungen 113
 - E-Mail- und SNMP-Statusmeldungen 77
 - Endbenutzerschnittstelle 97, 114
 - LDAP-Server 110
 - Nachrichtenspeicher 111
 - SMTP 112

- Erweiterte Parameter für Clusterreplikation 113
- Erweiterte Parameter für LDAP-Server 110
- Erweiterte Parameter für Nachrichtenspeicher 111
- erwünschte E-Mail 55

F

- Firewallkonfiguration 10
- Forward Path-Domänenprüfung 25
- FTP-Server
 - konfigurieren 63
- Funktionen vii

G

- Globale IP-Zugriffsliste 28
- Grenz-IP-Adressen 28, 29

H

- HELO-Domäne 35
- HELO-Domänenprüfung 25
- host_reputation.border_ips 29
- Hostreputationsfilter 33
- HTTPS 10

I

- IBM
 - Technische Unterstützung ix
- IBM Connections 14
- IBM Lotus Quickr 14
- IBM Unterstützungsportal ix
- ICAP 14
- ICAP-Server 14
- ICMP-Pingsignal 11
- Integration aktivieren 105
- Interne Maildomäne 11
- Interne Netzschnittstelle 16

K

- Kennwörter 12
- Konfigurationseinstellungen 9, 86
- Konfigurationssicherung 85
- Konfigurationssicherung verwalten, Seite 9, 86

L

- LDAP 59
- LDAP-Einbindung 59
- Lizenz 8
 - installieren 8
- Lizenzschlüssel 8
- Lizenzvereinbarung vii
- Lokale Domänen 27
- lokale Domänen hinzufügen 27
- Lotus Domino-Server
 - Benutzerauthentifizierung aktivieren 107

- Lotus Domino-Server (*Forts.*)
 - Fehlerbehebung, LDAP-Verbindung 107
 - Verbindung einrichten 107
- Lotus Notes-Zugriffsberechtigungen 106
- Lotus Protector for Mail Security
 - Barrierefreiheit 115
 - Befehlszeile ix
 - Bewertungsstatus 4
 - CPU-Auslastung 5
 - Dokumentations-Website vii
 - E-Mail-Datenverkehrsstatus 5
 - Festplattenspeicherplatz 5
 - Firewallkonfiguration 10
 - Kennwörter ändern 12
 - Lizenz 8
 - Lizenzvereinbarung vii
 - Neue Funktionen vii
 - Ressourcenstatus 5
 - Schutzstatus 3
 - Sicherung 9, 86
 - SMTP-Warteschlangen 43
 - Speicherauslastung 5
 - Startseite 3
 - Status aktualisieren 6
 - Systembelastung 5
 - Systemstatus 7
 - Technische Unterstützung ix
 - Zielgruppe vii
- Lotus Protector Manager 1
 - Navigationsfenster 1
 - Navigationsstrukturkategorien 1
 - Symbole 2
 - Zugriffsmodi 1

M

- Mail Security-Datenbank 89
- Makros 69
- Malware-Fernererkennung 3, 56
- Modus mit eingeschränktem Zugriff 2
- Momentaufnahmedatei 85
- Momentaufnahmedatei, Standardeinstellungen 85
- Momentaufnahmedateien
 - erstellen 9, 86
 - generieren 85
 - herunterladen 9, 86
 - hochladen 9, 86
 - löschen 9, 86
 - wiederherstellen 9, 86
- Momentaufnahmen 9, 85, 86
- msgstore.quarantine_domains 67
- MX-Einstellung 19
- MX-Eintrag 19

N

- Nachrichtenprotokoll
 - Nachrichten löschen aus 64
- Nachrichtenspeicher 65
 - aktive Abfragen 65
 - einrichten 64
- Nachrichtenverfolgung 73
- Nachrichtenverfolgung/
 - Berichterstellung 73, 82

- Network Time Protocol 13
- Netzeinstellungen
 - ändern 14
- Netzschnittstellen 15, 16
 - verwalten 14
- Neue Funktionen vii
- NOTES.INI 105
- notspam@kassel.ibm.com 65, 109
- NULL-Absender zulassen 24

O

- Ohne Hinweis löschen 28, 29, 30, 31, 33
- Opportunistisches TLS 26

P

- PEM-Format
 - für Zertifikate 40, 41, 42
- Phishing 53
- Postmaster-E-Mail-Adresse 11
- Produktdokumentation vii
- Protokolldateien
 - anzeigen 80
 - Blockierte E-Mail-Nachrichten 80
 - herunterladen 80
 - löschen 38

Q

- Quarantänebericht 67, 69
 - Absender-E-Mail-Adresse 11
 - auslösen 65
 - E-Mail-Schablone 67
 - Empfänger definieren von 69
 - inaktivieren 66
 - planmäßige Zustellung 62
 - Zeilenschablone 67
- Quarantänespeicher 64, 67, 69

R

- Registerkarte "Aktualisierungseinstellungen" 90
- Registerkarte "Empfangender SMTP" 27
- Registerkarte "Externe Schnittstelle" 15
- Registerkarte "Interne Netzwerkschnittstelle" 16
- Registerkarte "Vorlagen für Quarantäneberichte" 69
- Relais-Server hinzufügen 27
- Relay-Server 27
- Response-Objekte 57
- Responses 57
 - Anhang hinzufügen 57
 - Anhang löschen 57
 - BCC 57
 - Bedingung für Einstellen/Löschen 57
 - Feld ändern 57
 - Geschäft 57
 - Haftungsausschluss hinzufügen 57
 - Protokoll 57
 - senden an 57
 - umleiten 57
 - Verschlüsselung erforderlich 57

- Responses (Forts.)
 - Weiterzugebende Nachricht 57
- Ressourcennutzung 4
- Ressourcenstatus 5
 - CPU-Auslastung 5
 - Datenbank 5
 - Datenspeicher 5
 - Festplattenspeicherplatz 5
 - Nachrichtenspeicher 5
 - Speicherauslastung 5
 - Systembelastung 5
- Richtlinie des Domino-Administrator-desktops 105
- Richtlinieneinstellungen 47
- Richtlinienkonfiguration 47, 69
- Richtlinienobjekt
 - E-Mail-Speicher 64
- Richtlinienregeln 47, 69
 - Aktionen 47
 - Empfängerliste 47
 - hinzufügen 47
 - Senderliste 47
 - Übersicht 48
 - Vorbedingungen definieren 52
 - Zeitraumen definieren 51
- Rootkennwort 12
- Routing 17
 - Manuell konfigurieren 17
- Routing-Modus 16
- Routing-Vorrangstellung 16

S

- Schablone für Quarantänebericht 67
- Schutzstatus 3
 - Blockierung der IP-Adresse 3
 - Empfängerüberprüfung 3
 - erwünschte E-Mail 3
 - Konformität 3
 - Malware-Fernererkennung 3
 - Phishing 3
 - Spam 3
 - Virensignaturerkennung 3
 - weitere 3
 - ZLA NDR 3
 - ZLA Spam 4
- Seite "Administratorkennwort" 12
- Seite "Automatische Updates" 90
- Seite "Berichterstellung" 82
- Seite "Diagnosedatei" 80
- Seite "Mail Security-Richtlinienobjekte" 69
 - Registerkarte "FTP-Server" 63
- Seite "Netzwerk" 15, 16
- Seite "Routen" 17
- Seite "SMTP-Konfiguration" 27
- Seite "Uhrzeit" 13
- Seite "Updates und Lizenzierung" 8
- Seite mit Protokolldateien 80
- Selbst signierte Zertifikate 26
- Sender SMTP 35
- server.cert 40
- Sicherung 9, 63, 85, 86
 - vollständiges System erstellen 87
 - wiederherstellen 87
- Signaturmustererkennung 56
- SMTP 10

SMTP (Forts.)

- Beendigung der Verbindung 24
- DNS-Suche 24
- E-Mail-Nachrichten empfangen 23
- globale Einstellungen 11
- Headerfeldinformationen 25
- konfigurieren 11
- Max. Anzahl Empfänger pro Nachricht 23
- Max. Empfänger pro Verbindung 23
- Max. MTA-Hops 24
- NULL-Absender zulassen 24
- Portnummer 23
- Routing-Datenverkehr 19
- Verbindungszeitlimit 24
- Willkommensnachricht (Begrüßung) 25
- SMTP, ausgehend 19
- SMTP, eingehend 19
- SMTP, erweiterte Parameter 112
- SMTP-Fehlercode 30
- SMTP-Fehlernachricht 30
- SMTP-Konfiguration 23, 27
 - Analyse der Nullebene 31
 - Blockierliste 29
 - Einstellungen zu ausgehenden E-Mails 35
 - Empfängerüberprüfung 30
 - globale IP-Zugriffsliste 28
 - Hostreputationsfilter 33
 - IP-Adressen unter Quarantäne stellen 33
 - Phishing-Treffer 33
 - Protokollierung 35
 - Sender SMTP 35
 - Sender benachrichtigen 35
 - Spamtreffer 33
 - Spoolfehler 35
 - Transport Layer Security (TLS) 26
 - Unzustellbare E-Mail-Adresse 35
 - Unzustellbarkeitsberichte 35
 - Verweigerungsliste 28
 - Weiterleitung 35
 - Zulassungsliste 28
 - Zustellungsfehler, E-Mail-Adresse 11
 - Zustellungsverzögerung 35
- SMTP-Maildomäne 11
- SMTP-Protokollierung 23
- SMTP-Relay 20
- SMTP-Verbindung
 - TLS-Sicherheit testen von 42
- SMTP-Warteschlangen 43
 - E-Mail-Nachrichten anzeigen 45
 - erneutes Spoolen von E-Mail-Nachrichten 44
 - Fehlerbehebung 44
 - Warteschlange "frozen" 44
 - Warteschlange "local" 43
 - Warteschlange "sending" 43
 - Warteschlange "unchecked" 43
 - Warteschlange, resend 43
 - Zustellungsfehler 45
- SNMP 11
- SNMP-Get 75
- SNMP-Trap 75
- spam@kassel.ibm.com 65, 109

- Spam-Collector-E-Mail-Adressen
 - notspam@kassel.ibm.com 109
 - spam@kassel.ibm.com 109
- Spam-DNSBL-Server 71
- Spambewertungen 55
- Spamdatenflusssteuerung 71
- Spamheuristik
 - Heuristische Analyse 55
 - vordefinierten Schwellenwert 55
- Spamschutzupdates 89
- Spamsignaturen
 - aktualisieren 10
- Speicherauslastung 5
- SPF-Eintrag 53, 54
- Squid 3.x 14
- SSH 10
- Startseite 3
 - Statusleuchtanzeigen 3
- Statische Route
 - hinzufügen 17
- Statisches Internet Protocol 15
- Status aktualisieren 6
 - Antivirensignaturen 7
 - Bayes-Filter-Datenbank 6
 - CAL-Scripting 6
 - Firmware des Systems 6
 - Inhaltsfilterdatenbank (Mail) 6
 - Inhaltsfilterdatenbank (Web) 6
 - Phishingsignaturen 6
 - Signaturen der Spamschlüsselwortana-lyse 6
 - Spamheuristiksignaturen 6
- Statusmeldungen
 - E-Mail-Benachrichtigung 75
 - Empfänger definieren 77
 - SNMP-Benachrichtigung 75
- Support-Datendatei 80
- Systembelastung 5
- Systemsicherung 85
- Systemsicherungen verwalten, Seite 87
- Systemsicherungs- & Wiederherstellungs-
seite 85
- Systemstatus 7
 - Basissoftwareversion 7
 - Betriebszeitstatus 7
 - Firmware 7
 - Inhaltsanalyse-Bibliothek 7
 - letzte Sicherung 7
 - letzter Neustart 7
 - Netzschnittstellen 7
 - Systemzeit 7
 - verwendete IP-Adressen 7

T

- technische Unterstützung, IBM ix
- TGZ-Dateiformat 80
- TLS-Verbindung
 - testen 42
- TLS-Zertifikate
 - Format überprüfen von 42
 - hinzufügen zu 41
 - hochladen 39
 - installieren 40
 - Serverzertifikate 39
- Transport Layer Security (TLS)
 - immer versuchen 26

U

- Uhrzeiteinstellungen 13
- Umgekehrte DNS-Suche 24
- unchecked/processing 43
- Unter Quarantäne gestellte E-Mail-Nach-
richten 64, 65
- Updates
 - automatisieren 90
 - E-Mail-Sicherheit 89
 - E-Mail-Sicherheits-Datenbank 89
 - Spamschutz 89
 - Spamsignaturen 89
 - Systempakete 89
 - Virenschutz 89
- Updates für E-Mail-Sicherheit 10
 - ausführen 10

V

- Verschlüsselungs-TLS 26
- Verzeichnisobjekte 59
- Verzögerte E-Mail-Nachrichten 65
- Virenscanservices in Echtzeit 14
- Virensignaturerkennung 3
- Vollständige Systemsicherungen 87
- Vordefinierte Berichte 81
 - generieren 82
 - Tage, die der Bericht aufbewahrt
wird 82
 - Typen 81
 - Zeitplan konfigurieren 83
 - Zeitplanung 82

W

- Warteschlange "frozen" 44
- Warteschlange "local" 43
- Warteschlange "resend" 43
- Warteschlange "sending" 43
- Warteschlange "unchecked" 43
- Website zur technischen Unterstüt-
zung ix
- Weiterleitungsregeln 22
- When-Objekte 47, 51
- Who-Objekte 47, 49
 - Empfängerüberprüfung 49
 - SMTP-Abgleich 50
 - Überprüfen 50
- Who-Objekte, Typ 49, 50
 - Benutzer 49
 - E-Mail 49
 - Gruppe 49
 - Verbund, Who 49
 - Verzeichnis 49
- Wiederherstellung 85

Z

- Zeitplanobjekte 62
- Zertifikate
 - anfordern 26
 - Format überprüfen von 42
 - selbst signiert 39
 - selbst signierte zulassen 26
 - überprüfen 26

- Zertifikate hinzufügen 41
- Zertifikatsformat konvertieren 42
- Zertifizierungsstelle (CA = Certificate Au-
thority)
 - Zwischenzertifikat 41
- ZLA
 - siehe* Analyse der Nullebene
- Zulassungsliste löschen 97
- Zustellung von Quarantäneberichten 72,
95
- Zwischenzertifizierungsstelle 41



SC12-4542-01

